Digitale Schnittstelle – Phase II: Piloten

Abschlussbericht

im Auftrag von

Oesterreichs Energie

Brahmsplatz 3, A-1041 Wien

23. Januar 2026

consentec

Digitale Schnittstelle – Phase II: Piloten

Abschlussbericht

im Auftrag von

Oesterreichs Energie

Brahmsplatz 3, A-1041 Wien

23. Januar 2026

Consentec GmbH

Grüner Weg 1
52070 Aachen
Deutschland
Tel. +49 (2 41) 93 83 6-0
E-Mail: *info@consentec.de*
https://www.consentec.de

Inhaltsverzeichnis

1 Hintergrund

Der österreichische Branchenverband Oesterreichs Energie (OE) und seine Mitgliedsunternehmen befassen sich zurzeit mit Konzepten für die netz- und systemorientierte Nutzung von Flexibilitätspotenzialen bei den Netznutzern. In einem dieser Projekte befasst sich eine Projektgruppe von OE mit dem Thema „Digitale Schnittstelle (DSS)“. Dabei sollen Anforderungen an die technische Schnittstelle konzipiert werden, die für die Nutzung von Flexibilitätspotenzialen insbesondere bei kleineren Netzkunden – vorwiegend Verbrauchern, die aber auch über Erzeugungs- und Speicheranlagen verfügen können – benötigt werden. Dies ist relevant, da in diesem Bereich bisher in der Regel keine Kommunikationswege für die Flexibilitätsnutzung vorhanden sind, anders als z. B. bei größeren Erzeugungsanlagen oder auch großen Stromverbrauchern. Die Notwendigkeit, über eine geeignete Schnittstelle Steuer- und ggf. auch Preissignale für die Flexibilitätsnutzung übermitteln zu können, erstreckt sich bis hin zu den Haushaltskunden, da auch diese in Form von Wärmepumpen, E Pkw-Ladeeinrichtungen, Heimspeichern und anderen Verbrauchseinrichtungen in Zukunft zunehmend über relevante Flexibilitätsoptionen verfügen werden.

OE hat das Projekt DSS in drei Phasen unterteilt. In der Phase I wurden verschiedene Grundlagen zu Ausgangslage, Zielsetzungen, Rahmenbedingungen, Anwendungsfällen und technischen Realisierungsmöglichkeiten der digitalen Schnittstelle erarbeitet. In der sich anschließenden Phase II („DSS – Scope“) wurde herausgearbeitet, welche Kommunikationsbeziehungen und -prozesse zwischen den Akteuren im Stromsystem für die betrachteten Fälle der Flexibilitätsnutzung erforderlich sind und welche Anforderungen sich hieraus für die Ausgestaltung der digitalen Schnittstelle ergeben.

In der nun abgeschlossenen Phase II („Piloten“) wurden die zuvor erreichten Ergebnisse durch die enge Begleitung unterschiedlicher Pilotprojekte näher auf den Prüfstand gestellt. Hierzu wurden mehrere unterschiedliche Piloten initiiert und deren Erfahrungen bei der Auslegung des finalen Designs der digitalen Schnittstelle berücksichtigt.

Das Projekt hatte eine Laufzeit von gut anderthalb Jahren und wurde offiziell Dezember 2025 beendet. Teilweise wurden die Arbeiten in den Pilotprojekten über das Enddatum dieses Projektes hinaus weiter vorangetrieben.

In dem ersten Teil des Berichtes sind die während der Projektbearbeitung übergeordneten Schlussfolgerungen für das Design der DSS aufgeführt. Jeder Pilot wurde zum Projektabschluss gebeten, den Piloten näher vorzustellen sowie die für ihn bis zu diesem Zeitpunkt erzielten wesentlichen Erkenntnisse und Schlussfolgerungen für das Design der DSS zusammenzufassen. Diese Antworten sind in dem zweiten Teil des Abschlussberichtes aufgeführt.

2 Teil 1: Erkenntnisse und Festlegungen zum Zieldesign der DSS

2.1 Überblick über die Pilotprojekte

Insgesamt wurden 10 Pilotprojekte (Piloten) initiiert. In der untenstehenden Tabelle sind die Namen der Piloten, die beteiligten Netzbetreiber und die involvierten Industrieunternehmen aufgelistet.

Name des Piloten:	Netzbetreiber:	Industrieunternehmen:
Pilot 1: Datahub	Netz Oberösterreich	Gridoo, Loxone
Pilot 2: DSS	Linz Netz	Gridoo
Pilot 3: „Pilot 3a“	Energienetze Steiermark	Fronius International
Pilot 4: Cloud Gateway für Flexibilitäten	Netz Burgenland	Fronius International , Burgenland Energie, Hochschule Burgenland, Scheiber Solutions
Pilot 5: EnWG §14a	Voralberger Energienetze & e-netze Allgäu	PSI, Prolan, Voltaris, PPC
Pilot 6: INSIEME	Energienetze Steiermark	EDA, Enfor, Enlite
Pilot 7: EMMA	KNG-Kärnten Netz	Schneider Electric, Emulate
Pilot 8: Grid Stabilizer	Netz Niederösterreich	WAGO Kontakttechnik
Pilot 9: OpenGrid4PV	EWE & E-Werk Perg	Reisenbauer, Sticon
Pilot 10: Friendly Charge	Energienetze Steiermark	Montanuniversität Leoben, Technische Universität Wien, AIT Austrian Institute of Technology , Energie Steiermark, E-VO eMobility, Siemens Österreich

Tabelle 2.1: Übersicht der Pilotprojekte, Netzbetreiber und Industrieunternehmen

Die während der Projektlaufzeit betreuten zehn Pilotprojekte stellen eine große Bandbreite von unterschiedlichen Ansätzen und angesteuerten Netzgruppen dar und können somit als für Österreich repräsentativ angesehen werden. Die untersuchten steuerbaren Anlagen sind eine Kombination aus PV-Anlagen bzw. deren Wechselrichter, Heimspeicher, Ladepunkte für E-Mobilität und Wärmepumpen. Bei den Lösungen zum Ansteuern der flexiblen Verbraucher wurde teilweise zusätzlich Hardware beim Kunden verbaut, teils das Energie-Management-System (EMS) angesteuert und teils eine Kombination mit Cloud-Software verwendet. Auch bei der Kommunikation wurden Ansätze mit Mobilfunk oder dem kundeneigenen Internet erprobt.

Insgesamt ergibt sich eine große Heterogenität aus den Pilotgruppen, wodurch davon ausgegangen werden kann, dass die erzielten Erkenntnisse auf möglichst viele Einsatzwecke in der Praxis übertragen werden können. Die Einschätzungen der Pilotprojekte zu notwendigen Standardisierungen, sowie die sich ergebenen Herausforderungen und Empfehlungen bei der Einführung einer Digitalen Schnittstelle werden in den nachfolgenden Unterkapiteln stichpunktartig aufgeführt

2.1.1 Notwendige Standardisierungen

- **Interoperabilität statt Insellösungen:** Ohne Standards entstehen viele proprietäre Adapter je Hersteller/System → hoher Wartungsaufwand, mehr Komplexität und Kosten.
- **Verbindliche Schnittstellenspezifikation (MUSS/SOLL):** Präzise festlegen, welche Funktionen/Daten verpflichtend sind und welche optional (z. B. als Profil wie OpenADR 3.1) → weniger Interpretationsspielraum, geringeres Implementierungsrisiko.
- **Mandatory vs. Optional als Balance:** Verpflichtender Kern ermöglicht schnellen Start, optionale Erweiterungen sichern Zukunftsfähigkeit, ohne zu stark einzuschränken.
- **Einheitliches Protokoll & harmonisierte Datenmodelle:** Gleiche Semantik, Nachrichtenformate und Dateninhalte zwischen Netzbetreiber, Netznutzer und ggf. weiteren Marktteilnehmern sind Voraussetzung für Skalierung.
- **Harmonisierte Architekturvarianten:** Unterschiedliche regionale Umsetzungen erschweren Rollout und Skalierung → konsistente Architekturprinzipien (österreichweit, idealerweise EU-weit).
- **Standardisierte Portal-/API-Schnittstellen (DSS-Portal):** Einheitliche Anbindung für Hersteller, EMS, Aggregatoren und VNBs → weniger Integrationsaufwand.
- **Standardformate für Steuerung & Feedback:** Einheitliche Formate für Hüllkurven, Befehle und Rückmeldungen sind zentral für automatisierte, zuverlässige Steuerung
- **Sicherheits- & Authentifizierungsstandards:** Einheitliche Security-Mechanismen schaffen Vertrauen, Compliance und ermöglichen skalierbare Rollouts.
- **Standardisierte Prozesse (On-/Offboarding, Validierung):** Niedrige Eintrittsbarrieren (insb. für Aggregatoren) durch einheitliche Abläufe inkl. Prüf-/Validierungsprozessen.
- **Gleiche Grundfunktionalitäten bei jedem VNB:** Vergleichbare Basisfunktionen in allen Netzgebieten verhindern fragmentierte Anforderungen und hohe Integrationskosten.
- **Marktkommunikation mitdenken:** Standardisierung muss auch Kommunikationsbeziehungen zu Marktakteuren (Aggregator/Flexmarkt) abdecken.
- **Standard als Voraussetzung für Automatisierung (Netzverträglichkeit/Feedback-Loops):** Automatisierte Prüfungen und schnelle Rückmeldungen funktionieren nur mit standardisierten Daten, Formaten und Abläufen.
- **Dokumentation & Qualitätsanforderungen:** Einheitliche Anforderungen an Eingriffe, Dokumentation, Hard-/Software und Netzzustandsermittlung erhöhen Nachvollziehbarkeit und Betriebssicherheit.
- **Cloud-Anbindung – aber standardisiert:** Cloud kann funktionieren, wird aber erst durch Standards breit reproduzierbar und unabhängig von Einzellösungen.

2.1.2 Herausforderungen bei der Einführung von DSS

- **IT-Security & Regulierung als Bremsfaktor:** Hohe Sicherheitsanforderungen (IT/OT, z. B. sichere Broker/Kommunikation) plus regulatorische Klärungen binden Ressourcen und verzögern Projekte.

- **Datenschutz als Aufwandsblock:** Hoher Abstimmungsbedarf; länderspezifische Unterschiede verhindern einfache, einheitliche Prozesse/Referenzmodelle.
- **Interoperabilität & Integration in der Praxis schwierig:** Viele Gerätetypen/Hersteller-APIs, teils fehlende Dokumentation (z. B. Adapter), und oft kein IT-Zugang beim Endkunden.
- **Kommunikation & Performance:** Latenzen durch seltene Updates (z. B. 10-Min-Takt) und API-Probleme; stabile (nahe) Echtzeitdatenübertragung bleibt herausfordernd.
- **Feld-Infrastruktur aufwändig/fragil:** Unzuverlässige lokale Netzwerke; Controller-Installation erfordert häufig Elektriker; hoher Hardwareaufwand.
- **Begrenzte Steuerbarkeit/Granularität:** Teilweise nur indirekte Begrenzung möglich (z. B. über Wechselrichter-Maxleistung); „behind-the-meter" braucht EMS für zählpunktscharfe Vorgaben.
- **Failsafe/Fallback & Betrieb:** Robuste Fallback-Werte nötig; bei Kommunikationsausfall drohen sonst unerwartet hohe Leistungsgradienten und instabiles Verhalten.
- **Skalierbarkeit & Betriebskonzepte fehlen oft:** Standardisierte Prozesse, Monitoring/Störungsmanagement, skalierbare Cloudplattform sowie ausreichend Architektur- und Testzeit sind erforderlich.
- **Kosten & Aufwand hoch:** Hohe Entwicklungs-, Betriebs-, Wartungs- und Security-Kosten; ohne Vergütung entsteht zusätzlicher Mehraufwand (u. a. zentrale Stelle/Handling beim Netzbetreiber).

2.1.3 Empfehlungen bei der Einführung von DSS

- **Früh offene Standards festlegen und einheitlich umsetzen:** Standardisierte Protokolle möglichst früh integrieren und österreichweit konsistent (idealerweise EU-weit) umsetzen; Hersteller früh abstimmen.
- **OpenADR 3.1 konkret als Zielstandard definieren:** Nicht nur „OpenADR nutzen", sondern ein klares Profil + gemeinsame Zielarchitektur verbindlich festlegen.
- **Rollen, Schnittstellen und Fail-Safe verbindlich regeln:** Klare Verantwortlichkeiten und definiertes Fallback-/Fail-Safe-Verhalten reduzieren Betriebsrisiken.
- **Update-Intervalle verkürzen:** Häufigere Datenaktualisierung (z. B. ≤ 5 Minuten) verbessert Reaktionsfähigkeit und Wirksamkeit.
- **Minimale Kunden-Hardware:** Bei Standard-Haushalten möglichst keine zusätzliche Netzbetreiber-Hardware vor Ort; Geräte bevorzugt über harmonisierte Schnittstellen via Kunden-Internet ansprechen.
- **Technik nicht durch starre Vorgaben ausbremsen:** Entwicklung ermöglichen, aber Konzepte inkl. Hard-/Software zertifizieren (Qualitätssicherung ohne Innovationsstopp).
- **Netzzustandsermittlung & Qualitätskriterien definieren:** Anforderungen an Messdaten, Echtzeitfähigkeit und Ansteuerqualität klar festlegen.
- **Realistische Erwartungen:** Kurzfristig ist echte Echtzeit-Steuerung auf Basis von Echtzeit-Messwerten nicht realistisch → Roadmap entsprechend planen.

- **Rollout-Verbindlichkeit sinnvoll regeln:** Einführungspflicht in angemessenem Umfang definieren (damit Adoption nicht optional/zufällig bleibt).
- **Cloud-Ansätze pragmatisch nutzen – mit Vergütung:** Herstellerclouds bei passender Vergütung nutzen (schnell umsetzbar); ohne Vergütung ggf. zentrale Stelle, aber Mehraufwand für Netzbetreiber beachten; alternative WAN-Kanäle weiter ermöglichen.
- **Regulative Vergütung gesetzlich verankern:** Kosten, die real entstehen (Netzbetreiber/Hersteller), müssen angemessen vergütet werden.
- **Genug Zeit & robuste Betriebsfähigkeit einplanen:** Planung, Infrastrukturaufbau, Tests, Monitoring/Störungskonzepte, Datenschutzprozesse und skalierbare Cloudplattform von Anfang an berücksichtigen.
- **Stakeholder früh einbinden & Nutzen aktiv kommunizieren:** Regulatorik früh abstimmen und DSS als Chance für ein zukunftssicheres Verteilnetz positionieren.

Parallel zu der Durchführung der Pilotprojekte wurde das finale Design der DSS weiterentwickelt. Die zwischenzeitlich in der Pilotphase gewonnenen Erkenntnisse konnten dabei unmittelbar in die Designfestlegung einfließen.

2.2 Use-Cases der DSS

Im Projekt wurden die von der DSS zu übernehmenden Use-Cases inklusive des dabei notwendigen Datenaustauschs je Datenkategorie abgestimmt. In Summe soll die DSS fünf Use-Cases abdecken.

- Use-Case 1 - Unterstützung Netzzustandsanalyse: Die DSS wird zukünftig zu robusteren Netzzustandsanalysen beitragen, indem die DSS den Netzbetreibern Daten aus der Sphäre des Netzkunden sendet, die diesen Rückschlüsse auf die Netzauslastung ermöglicht. Zu den übermittelten Daten zählen sowohl Stammdaten der Anlage in der Sphäre des Endkunden, Echtzeitwerte sowie Zählwerte.
- Use-Case 2 - Unterstützung Maßnahmendimensionierung: In Netzengpasssituationen ist es Aufgabe der Netzbetreiber, die unter Berücksichtigung des geltenden Rechtsrahmens, effizienten Maßnahmen zur Behebung von Engpässen zu identifizieren. Die DSS kann hierbei unterstützen, indem sie den Netzbetreibern Daten übermittelt.
- Use-Case 3 - Steuerung von flexiblen Einheiten / Beeinflussung Anlagenverhalten: Ein wesentlicher Einsatzzweck der DSS wird zukünftig in der Steuerung von flexiblen Anlagen bzw. in der Beeinflussung des Anlagenverhaltens liegen. Die DSS übermittelt hierbei nicht unmittelbar Steuerungssignale an die flexiblen Einheiten, sondern arbeitet ausschließlich mit Leistungsvorgaben. Diese einzuhalten ist Aufgabe des Endkunden.
- Use-Case 4 - Monitoring von flexiblen Einheiten: Es ist absehbar, dass flexible Einheiten zukünftig nicht zu jeder Zeit völlig uneingeschränkt eingesetzt werden können, sondern sich den vorherrschenden Netzrestriktionen unterwerfen müssen. Hierzu sind bereits diverse Steuerungsinstrumente im Gespräch und auch schon im ElWG verankert. Der DSS wird daher zukünftig die Aufgabe zukommen, die Netzbetreiber bei dem Monitoring von unterschiedlichen Anlagen zu unterstützen.
- Use-Case 5 – Konformitätsüberprüfung: Losgelöst vom täglichen Betrieb wird es ebenfalls Aufgabe der DSS sein, bei Konformitätsüberprüfungen eingesetzt zu werden. So können Netzbetreiber bspw. durch ein periodisch ausgetauschtes Heartbeat-Signal nachvollziehen,

ob der Kommunikationskanal mit der DSS uneingeschränkt funktioniert oder das Verhalten der Endkunden bei Testsignalen überprüft werden.

Aus diesen 5 Use-Cases gehen unterschiedliche Anforderungen an den Datentransfer zwischen Netzbetreiber und der DSS hervor, die in folgender Tabelle aufgelistet sind.

	UC1 Netzzustandsanalyse	UC2 Maßnahmendimensionierung	UC3 Beeinflussung Anlagenverhalten	UC4 Monitoring	UC5 Konformitätsüberprüfung
Stammdaten	▪ Anlagendaten (bei meldepflichtigen Anlagen; z. B. Typ, Anschlussleistung, …)				
Plandaten	/	/	**VNB an DSS:** ▪ Wirkleistungslimitierung ▪ Fail-Save-Verhalten **DSS an VNB:** ▪ Quittierung ▪ Anlagenstatus ▪ Messwerte	▪ /	▪ /
Echtzeitwerte	▪ Anlagenstatus ▪ Netzkennzahlen ▪ Messwerte			▪	▪ Heartbeat Signal ▪ Verhalten bei Testsignalen / seitens Kommunikation zwischen VNB und DSS
Zählwerte	▪ Netzkennzahlen ▪ Messwerte	/	/	▪ Messwerte	▪ Messwerte ▪ Informationen zu Wartung, Sicherheitsupdates, Operating, Maintenance etc.

Tabelle 2.2: Aus den Use-Cases hervorgehende Anforderungen an den Datenaustausch zwischen VNB und DSS

Es ist ersichtlich, dass die Datenanforderungen nutzungsfallübergreifend für einzelne Datenkategorien teilweise identisch sind. Für die Umsetzung der DSS in der Praxis bedeutet dies, dass ein effizienter Datenaustausch gewährleistet werden kann, mit dem unmittelbar mehrere unterschiedliche Use-Cases bedient werden können.

2.3 Marktkommunikation

Es erscheint sinnvoll, dass in Situationen mit netzbedingten Beeinflussungen des Anlagenverhaltens nach Möglichkeit unterschiedliche Akteure von diesen Beeinflussungen informiert werden. Neben dem Endkunden umfasst dies auch weitere relevante Marktakteure, wie beispielsweise Lieferanten, Bilanzgruppenverantwortlichen oder (wirtschaftlichen und technischen) Aggregatoren, im Folgenden unter Marktkommunikation verstanden. Im Gegenzug können auch Marktakteure ein Interesse daran haben, die DSS als Kommunikationsmedium zu nutzen, um Informationen oder Steuersignale an die Endkunden zu senden.

Hierbei stellt sich die Frage, inwiefern die DSS bei der Marktkommunikation einbezogen werden soll. Während der Endkunde unmittelbar über die DSS die Informationen für die Beeinflussung des Anlagenverhaltens erhält, existieren für die Informationsweitergabe an die Marktakteure unterschiedliche denkbare Optionen, die im Rahmen des Projektes erörtert wurden.

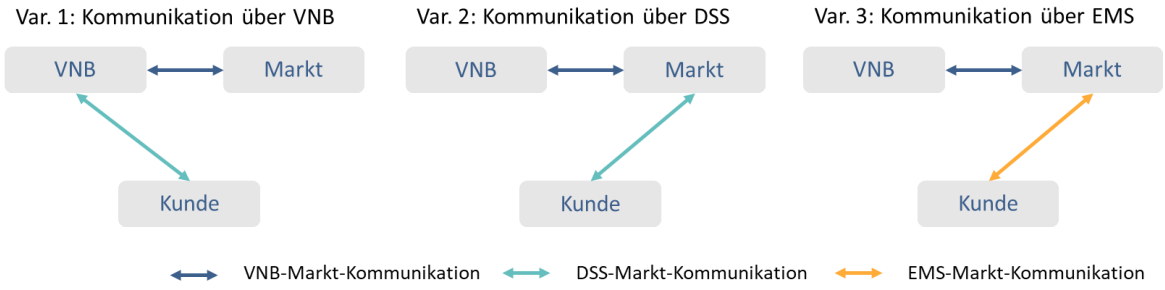


Abbildung 2.1: Möglichkeiten der Marktkommunikation

Eine Möglichkeit bestünde darin, dem VNB die Verantwortung zu übertragen, die relevanten Marktakteure zu informieren. In diesem Fall ist es Aufgabe der Netzbetreiber, in dezentralen Systemen eine stets aktuelle Zuordnung von Endkunden zu involvierten Marktpartner zu unterhalten und den Datenversand zu organisieren. Die DSS würde dabei nicht unmittelbar eingebunden werden, wodurch es bei dieser Variante nur geringe Auswirkungen auf das Design der DSS geben würde. Allerdings müsste sichergestellt werden, dass die DSS in der Lage ist, alle Informationen bzw. Steuersignale, die Marktteilnehmer an den Endkunden senden wollen, zu übertragen.

Grundsätzlich ist vorstellbar, dass die Kommunikation direkt zwischen den Marktakteuren und der DSS durchgeführt wird. In diesem Fall müsste dezentral in der DSS die Informationen über die involvierten Marktakteure vorgehalten und verwaltet werden. Die Kommunikation könnte in dieser Variante ohne Einbindung des VNB erfolgen.

Eine bereits heute etablierte Praxis liegt in der Nutzung der beim Kunden installierten Energiemanagementsysteme (EMS). In dieser Variante würde das EMS beim Kunden genutzt, die über die DSS eingehenden Signale und Informationen an die Marktakteure weiterzuleiten. In dem EMS müsste hierzu eine entsprechende Verwaltung der relevanten Marktakteure stattfinden. Eine Übermittlung von Informationen oder Steuersignalen seitens der Marktakteure könnte ohne Involvierung der DSS und der VNB erfolgen.

Es ist nicht Aufgabe noch im Interesse der VNB, eine Marktkommunikation über das EMS zukünftig zu unterbinden und eine Kommunikation ausschließlich über die DSS als Standard vorzusehen. Entsprechend ist davon auszugehen, dass eine Einbindung der EMS bei den Endkunden zukünftig ohnehin erfolgen wird. Demnach soll für Kunden, die heute oder zukünftig über ein EMS verfügen, diese Option weiterhin zugelassen werden.

Es können aber Fälle nicht ausgeschlossen werden, in denen die Kunden über kein EMS verfügen, allerdings flexible Einheiten (Wallbox, PV-Anlagen, …) und auch eine DSS installiert sein werden. Entsprechend muss auch für solche Fälle ein Kommunikationsstandard etabliert werden. Die Netzbetreiber haben sich dafür ausgesprochen, für solche Fälle eine Kommunikation über den VNB durchzuführen (Variante I). In der Variante II (Kommunikation über DSS) wird insbesondere als nachteilig angesehen, dass die DSS Kommunikationskanäle zu Marktakteuren aufbauen müsste und eine dezentrale Verwaltung der Daten der Marktakteure stattfinden müsste.

2.4 Kommunikationsprotokoll

Das Kommunikationsprotokoll zwischen VNB und DSS und vermutlich auch den Marktakteuren stellt bislang ein weiteres fehlendes Puzzleteil zur finalen Designfestlegung der DSS dar. Das Ziel besteht in der Definition eines österreichweit einheitlichen Kommunikationsprotokolls, das sämtliche identifizierten Anforderungen an die DSS erfüllt und dabei die Vorgaben der Marktkommunikation berücksichtigt. Eine solche Standardisierung ist wesentliche Voraussetzung für Investitionssicherheit sowohl auf Seiten der Hersteller als auch der Netzbetreiber.

In der Phase I des Projektes wurden bereits durch das AIT mehrere Standards und Protokolle aus dem Smart Grid Bereich bewertet, die bei einer bidirektionalen digitalen Schnittstelle zum Einsatz kommen könnten. Das Ergebnis der Studie ist in nachfolgender Tabelle noch einmal wiedergegeben. Die tabellarische Darstellung der Protokollvergleichs zeigt eine Favorisierung von IEEE 2030.5 sowie OpenADR.

	Generell	Operativ	Technologie-spezifisch	Security	**Summe**
IEEE 2030.5	+	+	++	++	**++**
IEC 62746 (OpenADR)	+	+	++	++	**++**
IEC 61850	+	+	++	++	**+**
DNP3	+	++	+	+	**+**
IEC 60870-104	+	~	+	+	**+**

Tabelle 2.3: Bewertung der Standards und Protokolle für die zentrale VNB-Schnittstelle, gewichtet (Quelle OE Phase I-Bericht zur bidirektionalen Digitalen Schnittstelle)

Beide der favorisierten Protokolle sind grundsätzlich in der Lage, die Anforderungen an die DSS zu erfüllen. In den Pilotprojekten wird allerdings weit überwiegend ein Kommunikationsprotokoll eingesetzt, die von diesen favorisierten Protokollen abweicht. Entsprechend ist nicht für jedes Protokoll mit belastbaren Erfahrungen aus den Piloten zu rechnen. Vor diesem Hintergrund besteht für Österreich ein zeitnaher Entscheidungsbedarf hinsichtlich des Kommunikationsprotokolls zwischen VNB und DSS. Zur fundierten Entscheidungsfindung wurde im Rahmen des Projektes ein Deep-Dive initiiert und eine entsprechende Task-Force eingerichtet, die von ATB und Fronius geleitet wurde.

Die Taskforce hat dabei identifiziert, mit denen die beiden favorisierten Protokolle IEEE 2030.5 und OpenADR bewertet werden konnten. Bei OpenADR wurde zwischen OpenADR 3.0 und OpenADR 3.1 differenziert.

Kriterium	IEEE 2030.5	OpenADR 3.0	OpenADR 3.1
Polling notwendig?	Ja	Ja	Nein (MQTT)
Latenzzeit durch Polling?	Ja	Ja	Nein
Direkte Aktionsauslösung durch Netzbetreiber?	Eingeschränkt	Eingeschränkt	Ja
Datenmenge im Betrieb	Hoch durch Polling (außer Aggregator-Clients)	Hoch durch Polling	Reduziert durch MQTT
Subscription/Notification möglich?	Ja, meist bei Aggregatoren	Nur mit Webhooks	Ja, via MQTT
Skalierbarkeit (VEN/Clients)	Keine Protokollgrenzen	Keine Protokollgrenzen	Keine Protokollgrenzen
Zertifikats- und PKI-Flexibilität	Eigene CA möglich	Eigene CA möglich	Eigene CA möglich
Clientzertifikate möglich?	Ja	Ja	Ja
Nachrichten einzeln signierbar?	Möglich	Möglich, aber selten genutzt	Möglich
Implementierungsaufwand (Client)	Einfach (REST/XML)	Einfach (JSON)	Einfach (JSON)
Implementierungsaufwand (Server)	Mittel bis hoch	Mittel	Mittel
Verfügbarkeit von Testtools	Kommerzielle Tools verfügbar	Online-Tool verfügbar	Online-Tool verfügbar
Verfügbarkeit von Softwarebibliotheken	XML-basierte Stacks, Open Source & kommerziell	Python, Rust (Open Source)	Python, Rust (Open Source)
Flexibilität für eigene Profile	Ja	Ja	Ja
Abbildung DSS-Basisfunktionalität	Möglich	Möglich	Möglich

Tabelle 2.4: Ergebnisse der Taskforce zur finalen Auswahl des Kommunikationsprotokolls.

Im Ergebnis dieses Vergleichs zeigt sich, dass sowohl OpenADR als auch IEEE 2030.5 grundsätzlich geeignet sind, die Anforderungen an die DSS zu erfüllen. OpenADR 3.0 und IEEE 2030.5 sind dabei als funktional gleichwertig zu bewerten. OpenADR 3.1 ist jedoch aufgrund der Integration von MQTT aus heutiger technischer Sicht als vorzugswürdig einzustufen. Dies gilt insbesondere für das nicht mehr notwendige Poling, die Möglichkeit der direkten Aktionsauslösung durch die Netzbetreiber sowie auch des niedrigen Bedarfs an Datenmengen.

Ob und wann IEEE 2030.5 künftig ebenfalls auf MQTT setzen wird, ist derzeit nicht abschätzbar; ein konkreter zeitlicher Rahmen ist nicht absehbar. Die Entwicklung von OpenADR 3.1 ist hingegen abgeschlossen, und der Standard steht bereits als Paket zum Download zur Verfügung. OpenADR 3.1 wurde daher als Kommunikationsprotokollstandard festgelegt.

2.5 Kommunikationsmedium

Das Kommunikationsmedium mit der DSS beim Endkunden wurde in den Vorgängerprojekten bislang nicht vertieft analysiert und auch im vorliegenden Projekt bisher nur unzureichend betrachtet. Gleichzeitig ist fraglos, dass die Kommunikation mit der DSS auf einem geeigneten Kommunikationsmedium aufsetzen muss, um einen stabilen, sicheren und wirtschaftlichen Betrieb zu ermöglichen.

Für die Bewertung geeigneter Kommunikationsmedien sind mehrere Kriterien maßgeblich. Dazu zählen insbesondere die erreichbare Latenz, die Wirtschaftlichkeit der Lösung, die Vereinbarkeit mit einem schnellen Rollout, die verfügbare Bandbreite, die technische und organisatorische Komplexität, die Anfälligkeit gegenüber Störungen, die Sicherheit, die Marktdurchdringung beziehungsweise Verfügbarkeit sowie der Aufwand für das Onboarding.

Als grundsätzlich mögliche Kommunikationsmedien kommen unter anderem Smart-Meter-Gateways, Breitband-Internetanschlüsse (z. B. DSL oder Glasfaser), Mobilfunklösungen (LTE/5G inklusive 450-MHz-Frequenz), Powerline Communication (PLC), Funklösungen wie LoRaWAN sowie sonstige Direktverbindungen, etwa auf Basis von MPLS, in Betracht.

Vor diesem Hintergrund stellt sich die zentrale Fragestellung, ob für die Kommunikation mit der DSS ein österreichweit einheitliches Kommunikationsmedium vorgegeben werden soll. Aus Sicht der Netzbetreiber erscheint die ausschließliche Verwendung eines einzigen Kommunikationsmediums nicht mit den zuvor dargestellten Bewertungskriterien vereinbar. Gleichwohl wird eine gewisse Vereinheitlichung als sinnvoll erachtet, um Homogenität in Prozessen und technischen Entwicklungen sicherzustellen. Da keine der betrachteten Lösungen flächendeckend einsetzbar ist und gleichzeitig alle Kriterien erfüllt, wird vorgeschlagen, ein möglichst einheitliches Kommunikationsmedium zu definieren, ohne alternative Lösungen grundsätzlich auszuschließen.

In einem weiteren Schritt wurde die Frage adressiert, ob das Internet als Kommunikationsmedium für die DSS empfohlen werden sollte. Nach Einschätzung der Netzbetreiber erfüllt das Internet die zuvor genannten Kriterien in ausreichendem Maße. Die Frage, ob Internet-basierte Kommunikation als hinreichend sicher einzustufen ist – insbesondere vor dem Hintergrund der entsprechenden Diskussionen in Deutschland – sollte gegebenenfalls durch eine dafür zuständige Stelle vertieft geprüft und bewertet werden.

Als Ergebnis schlagen die Netzbetreiber vor, das Internet als Standard-Kommunikationsmedium für die DSS festzulegen und in jenen Fällen, in denen eine sinnvolle Umsetzung nicht möglich ist, auf alternative Lösungen zurückzugreifen. Diese Positionierung wird weiterhin von

2.6 Architekturgrundzüge

Aufsetzend auf den zuvor getroffenen Festlegungen ergibt sich für die DSS die folgende Architekturlösung.

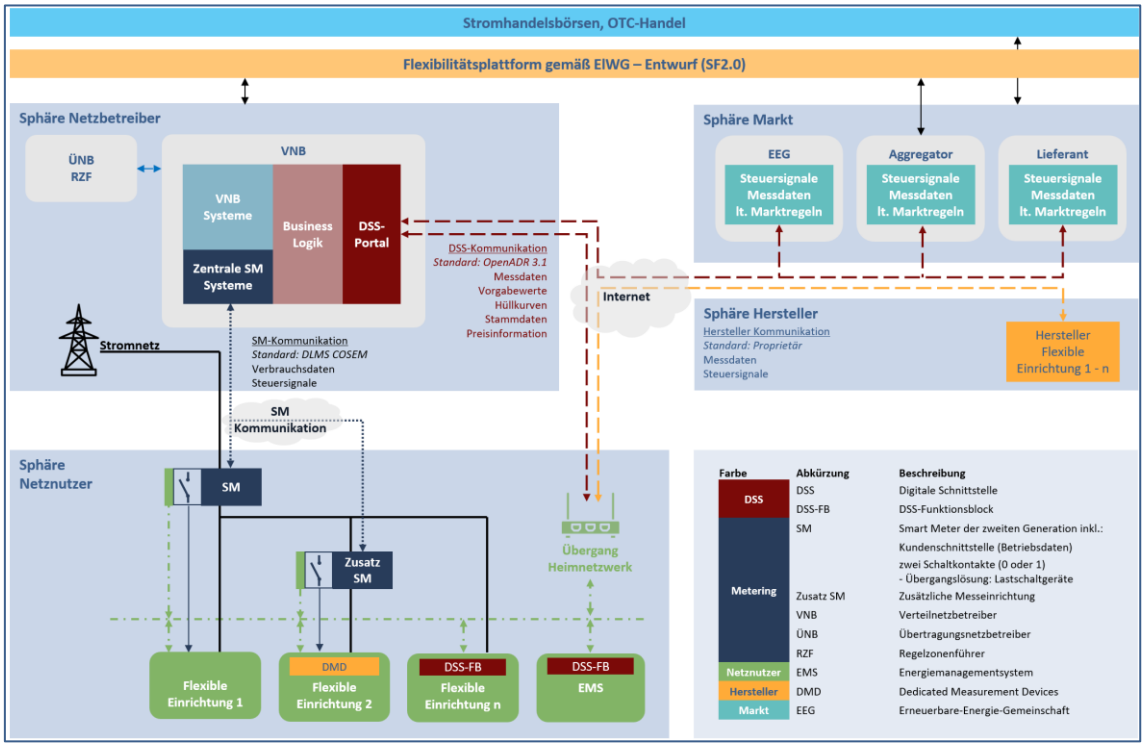


Abbildung 2.2: Erarbeitete Architekturlösung für die DSS

Die vorgeschlagene Architektur sieht vor, dass Netzbetreiber keine zusätzliche Hardware in den Kundenanlagen benötigen. Die Kommunikation der Kunden mit dem jeweiligen Anschlussnetzbetreiber erfolgt für klar definierte Zwecke vorzugsweise über das Internet. Alternativ können – abhängig von den örtlichen Gegebenheiten – auch andere Kommunikationswege wie LTE 450 oder sonstige Mobilfunklösungen eingesetzt werden.

Die Verantwortung für die ordnungsgemäße Umsetzung und den Betrieb der DSS-Funktionalität innerhalb der Kundenanlage liegt beim Kunden selbst. Kommt es zu einem Ausfall der Kommunikation zwischen Kunde und Anschlussnetzbetreiber, wird ein definiertes Fail-Safe-Verhalten aktiviert. Dieses stellt sicher, dass die Anlage in einen sicheren Betriebszustand übergeht, beispielsweise durch eine verminderte Einspeisung oder einen reduzierten Bezug.

Der Netzbetreiber ist für die Funktionalität und den Betrieb des DSS-Portals (Utility Server) verantwortlich. Die Marktkommunikation kann dabei optional über dieses DSS-Portal abgewickelt werden, ohne zwingend darauf angewiesen zu sein.

Die beschriebene Architektur ist konsistent mit dem Smart Meter Companion Standard sowie mit den Konzepten der Systemführung 2.0 und der EP-Flexibilitäten abgestimmt und fügt sich damit in die bestehenden und geplanten energiewirtschaftlichen Rahmenwerke ein.

3 Teil 2: Berichte der Pilotprojekte

3.1 Erfahrungen der Pilotprojekte

Für diesen Abschlussbericht wurde von jedem Piloten ein Fragebogen ausgefüllt. Darin beschreibt jeder Pilot das Projekt, stellt es in einem Schaubild dar und nennt die aus seiner Sicht relevantesten in dem Pilotprojekt erzielten Erkenntnisse. Bei einem Teil der Piloten werden, im Anschluss an die Standardfragen, noch einige projektspezifische Fragen beantwortet.

Ein Überblick der Standardfragen, die von allen Piloten beantwortet wurden, ist in nachfolgender Aufzählung gegeben:

- Welche Zielsetzungen wurden verfolgt?
- Welche Architekturvariante in der Schnittstelle zum Kunden wurde umgesetzt?
- Auf welche flexiblen Einheiten wurde Einfluss genommen?
- In welcher Form wurden die flexiblen Einheiten angesteuert?
- Über welches Kommunikationsmedium wurde die DSS angebunden?
- Wie wurde die DSS beim Kunden installiert?
- Welche Daten wurden zu welchem Zeitpunkt über die DSS ausgetauscht?
- Gab es eine Quittierung seitens der Netzkunden?
- In welcher Granularität wurden Daten ausgetauscht?
- Wurden Anforderungen an Cybersecurity betrachtet und welche Art der Authentifizierung gab es?
- Wurden mehrere gegenläufige Steuersignale / Einsatzinformationen getestet? Wenn ja, welche Prioritätsregeln wurden definiert?
- Wo findet die Koordinierung der flexiblen Einheiten statt?
- Welches Monitoringkonzept wurde berücksichtigt? Wie konnte bspw. sichergestellt werden, dass die von einer flex. Einheit angeforderte netzdienliche Leistung auch am Zählpunkt angekommen ist?
- Welches Update-Management ist bei der angestrebten Lösung vorgesehen bzw. denkbar? Sind Funktionserweiterungen möglich? Welche Akteure müssten eingebunden werden?
- Wie resilient / robust ist die angestrebte Lösung, insb. mit Blick auf den Ausfall kritischer Infrastruktur bzw. wichtiger Komponenten? Kann ein Teilbetrieb aufrecht erhalten werden (z. B. bei dezentralen Ansätzen)? Welche Rückfallebenen sind in Situationen mit Störungen vorgesehen? Welche Fall-back-Prozesse wurden definiert? Wie anfällig ist das Lösungskonzept mit Blick auf Manipulationen, bspw. mit Blick auf ungewünschtes Netznutzerverhalten?
- Mit Blick auf die DSS: Wo werden Standardisierungsnotwendigkeiten gesehen?
- Welche Herausforderungen sind aufgetreten? Welche Empfehlungen für die Einführung einer DSS leiten Sie aus dem Piloten ab?

3.1.1 Pilot 1: Datahub für Netz OÖ

Involvierte Industrieunternehmen: Gridoo, Loxone

Laufzeit: März 2024 bis Sept. 2026

Beschreibung des Projektes:

Zielsetzung des Pilotprojektes war die Einrichtung, bzw. Erprobung einer Kommunikationsschnittstelle zwischen Verteilnetzbetreiber (VNB) und Energie Management Systemen (EMS) von Netzkunden. Eine direkte Ansteuerung von Verbrauchern oder Endgeräten war explizit kein Ziel des Projektes.

Auf Seiten des VNB wurde ein virtueller Linux-Server als zentrale Kommunikationsplattform eingerichtet. Dieser hostet einen MQTT-Broker und eine MySQL-Datenbank zur Verwaltung von Konfigurationsdaten sowie eine Influx DB zur Speicherung von Messwerten aus den Kundenanlagen.

Dieser Datahub stellt eine standardisierte Rest-API zur Verfügung, über die sowohl Konfigurationen vorgenommen als auch Daten ausgetauscht werden können. (z.B. Steuerbefehle, Hüllkurven, Messwerte, Meldungen, …)

Prozess der Kundenregistrierung (Erfolgt derzeit noch manuell)

Die Verknüpfung erfolgt über die Seriennummer des EMS beim Kunden: Mit einem API-Befehl werden dafür im DataHub a) die nötigen Einträge in Datenbanken und MQTT-Broker erstellt sowie b) die Zugangsdaten für das EMS generiert. Nach Eingabe dieser Zugangsdaten verbindet sich das EMS automatisch zum Datahub beim VNB.

Ablauf Kommunikation (Erfolgt derzeit noch manuell)

Wenn in einem bestimmten Bereich (Trafostation / Strang) die Leistungsaufnahme reduziert werden soll, sieht der Ablauf technisch gesehen wie folgt aus:

1. Betriebsführung identifiziert den Bedarf, die Einspeiseleistung in einem bestimmten Netzbereich auf maximal 70% zu begrenzen
2. Die Business-Logik des VNB generiert daraufhin ein entsprechendes Abregelungskommando und übermittelt dieses über Rest-API an den Datahub
3. Der Datahub veröffentlicht (published) das Kommando auf das jeweilige MQTT-Topic
4. Die EMS in den betroffenen Haushalten empfangen die Nachricht über das abonnierte MQTT-Topic
5. Die EMS setzen die übermittelten Vorgaben lokal um

Zusätzlich können Marktteilnehmer direkt an den MQTT-Broker angebunden werden, um eine standardisierte und bidirektionale Kommunikation zwischen Marktteilnehmer, Datahub und Netzkunden zu ermöglichen.

Kundenseitige Systemarchitektur

Auf Kundenseite kommt ein Energiemanagementsystem (z.B. Gridoo Brain, oder Loxone Miniserver) zum Einsatz.

Durch die Standardisierung des Kommunikationsprotokolls zwischen VNB und Kundenanlage (OpenADR 3.1) kann zukünftig eine weitgehende Herstellerunabhängigkeit für Energiemanagement-Einrichtungen erzielt werden.

Schaubild der Kommunikation zwischen den Akteuren:

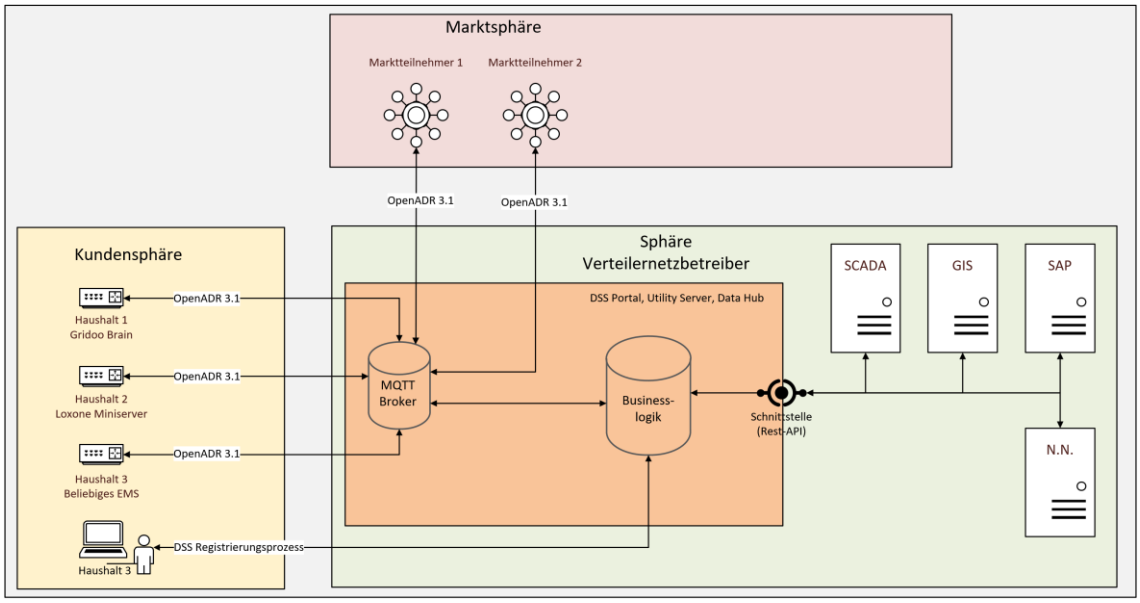


Abbildung 3.1: Schaubild von Pilot Datahub

Welche Zielsetzungen wurden verfolgt?

Sichere und standardisierte Kommunikationsschnittstelle zwischen Verteilnetzbetreiber und EMS des Netzkunden. Dadurch sollen z.B. VNB-seitig Leistungsgrenzen vorgegeben und relevante Messwerte beim Kunden ausgelesen werden.

Welche Architekturvariante in der Schnittstelle zum Kunden wurde umgesetzt?

Funktionsblock: Hardware mit eigener Software

Auf welche flexiblen Einheiten wurde Einfluss genommen?

Bis jetzt 2 Stück Test-Hardware: 1x Gridoo Brain und 1x Loxone Miniserver

Ziel: 10 Stk. Gridoo Brain

In welcher Form wurden die flexiblen Einheiten angesteuert?

Gesamtheit der flexiblen Einheiten in einer Anlage

Über welches Kommunikationsmedium wurde die DSS angebunden?

Application-Layer: Secure-MQTT, Transport-Layer: TCP

Anbindung über Internet / System gehostet bei NOOE

Wie wurde die DSS beim Kunden installiert?

Derzeit noch in Testumgebung. Keine Elektro-Installation beim Kunden notwendig. EMS kommuniziert über Kundennetzwerk mit den flexiblen Einheiten.

Welche Daten wurden zu welchem Zeitpunkt über die DSS ausgetauscht?

Leistungsvorgaben sowohl präventiv als auch kurativ (Einspeiseleistung & Verbrauch), Übertragung von aktuellen Leistungsdaten.

Gab es eine Quittierung seitens der Netzkunden?

Derzeit keine klassische Empfangsbestätigung. Bestätigung erfolgte über Messwert.

In welcher Granularität wurden Daten ausgetauscht?

Derzeit werden Echtzeitdaten übermittelt, die Latenzzeit beträgt < 3 Sekunden. Genauere Spezifikation ist noch notwendig, grundsätzlich über MQTT alles umsetzbar.

Wurden Anforderungen an Cybersecurity betrachtet und welche Art der Authentifizierung gab es?

Authentifizierung über ID + PW + Zertifikat. Die Kommunikation erfolgt über Secure-MQTT (MQTTS), das auf TLS-Verschlüsselung basiert. Damit wird etwaige Manipulation während der Übertragung verhindert, bzw. ist Integritätsschutz gegeben.

Zusätzlich können auf MQTT-Topic-Ebene die Teilnehmer nur auf die für sie relevanten Daten zugreifen.

Wurden mehrere gegenläufige Steuersignale / Einsatzinformationen getestet? Wenn ja, welche Prioritätsregeln wurden definiert?

Wurde zu diesem Zeitpunkt noch nicht genauer betrachtet. Derzeit erfolgen Vorgaben nur durch den Netzbetreiber.

Wo findet die Koordinierung der flexiblen Einheiten statt?

Koordinierung der flexiblen Einheiten erfolgt im EMS (z.B. Gridoo Brain, Loxone Miniserver)

Welches Monitoringkonzept wurde berücksichtigt? Wie konnte bspw. sichergestellt werden, dass die von einer flex. Einheit angeforderte netzdienliche Leistung auch am Zählpunkt angekommen ist?

Es wurde noch kein fixes Monitoringkonzept definiert. Es ist möglich, Leistungswerte zu monitoren.

Welches Update-Management ist bei der angestrebten Lösung vorgesehen bzw. denkbar? Sind Funktionserweiterungen möglich? Welche Akteure müssten eingebunden werden?

Weder VNB- noch kundenseitig ein Problem. Serverseitige Anpassungen jederzeit möglich, EMS-Updates sind über Firmware-Updates der jeweiligen Hersteller vorgesehen.

Wie resilient / robust ist die angestrebte Lösung, insb. mit Blick auf den Ausfall kritischer Infrastruktur bzw. wichtiger Komponenten? Kann ein Teilbetrieb aufrecht erhalten werden (z. B. bei dezentralen Ansätzen)? Welche Rückfallebenen sind in Situationen mit Störungen vorgesehen? Welche Fall-back-Prozesse wurden definiert? Wie anfällig ist das Lösungskonzept mit Blick auf Manipulationen, bspw. mit Blick auf ungewünschtes Netznutzerverhalten?

Bei Ausfall von zentralen Systemen sind Fallback-Werte (Fail-safe-Verhalten) in den Anlagen definiert. Bei Ausfall von dezentralen Komponenten ist die Wirkung auf das Gesamtsystem vernachlässigbar.

Mit Blick auf die DSS: Wo werden Standardisierungsnotwendigkeiten gesehen?

Entscheidend ist eine genaue Definition der gewünschten (MUSS / SOLL) Möglichkeiten in Bezug auf OpenADR 3.1. Dies sollte in einer Schnittstellenspezifikation definiert werden. Unbedingt zu beachten ist in diesem Zusammenhang auch die Berücksichtigung der Kommunikation von Marktteilnehmern.

Welche Herausforderungen sind aufgetreten? Welche Empfehlungen für die Einführung einer DSS leiten Sie aus dem Piloten ab?

Entscheidend ist eine fix definierte, gemeinsame Zielarchitektur. Weiters ist eine genaue Definition des OpenADR 3.1 Protokolls als „Österreich Standard“ entscheidend.

3.1.2 Pilot 2: DSS für Linz Netz

Involvierte Industrieunternehmen: gridoo

Laufzeit: 11/2024 bis 06/2026

Beschreibung des Projektes:

Ziel war die **Implementierung einer skalierbaren Kommunikationslösung** für die Vorgabe von Leistungsgrenzen aus der Sphäre des VNB an einzelne oder gruppierte Kundenanlagen.

Diese Leistungsgrenzen können auf Viertelstundenbasis und getrennt für Einspeisung und Bezug vorgegeben werden. Es sind **präventive** Vorgaben (Hüllkurven für die nächsten Tage) und **kurative** Eingriffe (sofort umsetzen) möglich.

Sicherheitsaspekte wurden von Anfang an berücksichtigt, um die Praxistauglichkeit für einen möglichen späteren Normalbetrieb zu prüfen.

Das Projekt besteht aus 2 Teilen:

1. **Kundenseitig** ist jeweils ein gridoo Brain (EMS) inklusive gridoo Eye (Smart Meter Auslesung) verbaut. Diese Komponenten sind entweder im/beim Verteiler eingebaut oder als Tischvariante in Verwendung (die Smart Meter der Linz Netz arbeiten mit wireless M-Bus, es ist also keine Kabelverbindung nötig). Die Kommunikation mit dem VNB erfolgt entweder über das Internet des Kunden (Wifi oder Netzwerkanschluss) oder über ein separates LTE-Modem.
2. **Auf Seite des VNB** ist eine Serverapplikation (gridoo dataHub) mit folgenden Aufgaben im Einsatz:
   - Authentifizierung und die laufende Kommunikation mit den Kundenanlagen
   - Aufbereitung und Speicherung von Echtzeitdaten in internen Datenbanken
   - Zuordnung von Kundenanlagen (Brain X gehört zu Kunde Y) und Verwaltung von Gruppen (zB alle Anlagen mit PV hinter Trafo xy)
   - Kommunikationsschnittstelle (REST-API) zur Leitebene der Linz Netz, über die DSS-Kommandos generiert und versendet werden

Die Umsetzung der DSS-Kommandos liegt in der Verantwortung des gridoo Brain und erfolgt entweder digital (zB Modbus) oder über zwei integrierte potentialfreie Relaiskontakte (Abschaltung der PV-Inverter oder von Verbrauchern, wie zB einer Ladestation).

Beim erstmaligen Anschluss eines gridoo Bain wird automatisch eine sichere **Websocket-Verbindung (TLS)** zum VNB aufgebaut.

Im Falle einer Übernahme des Piloten in den laufenden Betrieb ist eine Umstellung der Kommunikation auf **MQTT/openAdr 3.1** mittels OTA-Update möglich.

Schaubild der Kommunikation zwischen den Akteuren:

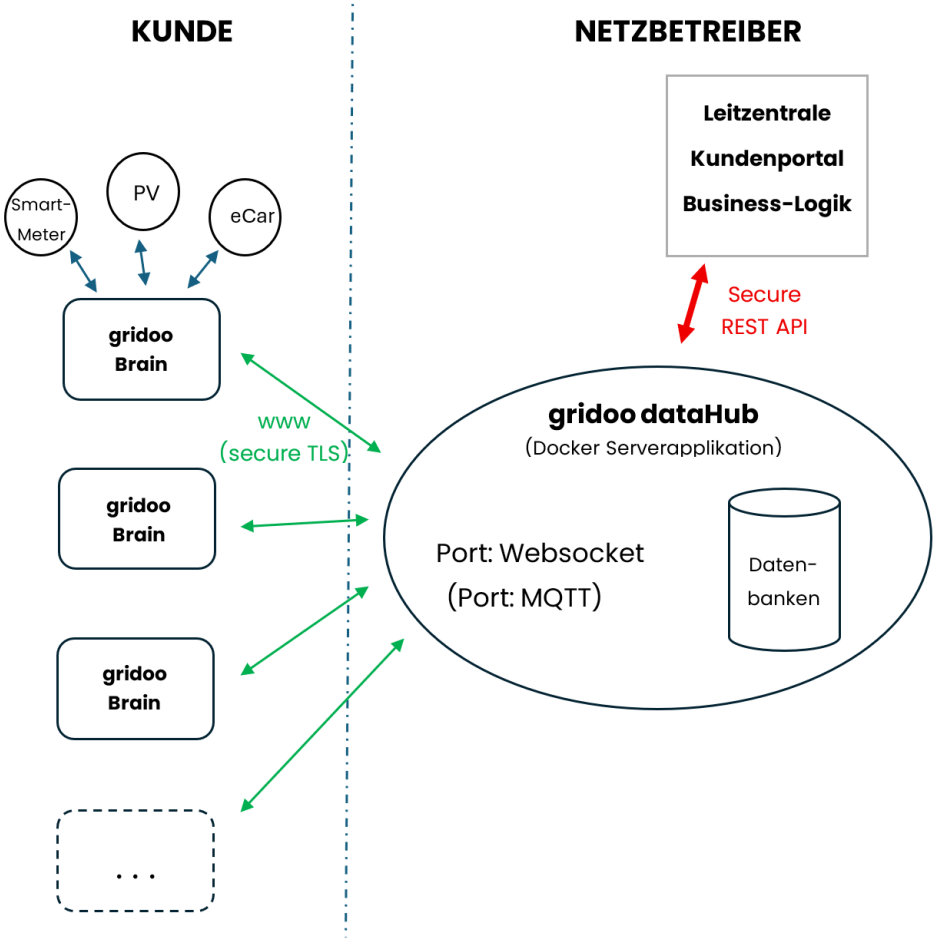


Abbildung 3.2: Schaubild von Pilot DSS

Welche Zielsetzungen wurden verfolgt?

Skalierbare Lösung für a) die Limitierung der Leistung am NAP in beide Richtungen und b) die Erfassung von Echtzeitdaten.

Welche Architekturvariante in der Schnittstelle zum Kunden wurde umgesetzt?

Funktionsblock: Hardware mit eigener Software

Auf welche flexiblen Einheiten wurde Einfluss genommen?

PV-Inverter und Ladestationen; Final sind 8 Kundenanlagen vorgesehen

In welcher Form wurden die flexiblen Einheiten angesteuert?

Gesamtheit der flexiblen Einheiten in einer Anlage und Einzelne flexible Einheit einer Anlage (beide Varianten werden eingesetzt)

Über welches Kommunikationsmedium wurde die DSS angebunden?

Internetverbindung über ein eigenes LTE-Modul oder über das Kundeninternet (Wifi oder Netzwerkanschluss des gridoo Brain)

Wie wurde die DSS beim Kunden installiert?

Aufgabe von gridoo. gridoo Brain (EMS) und gridoo Eye (Auslesen der Smart Meter) als Reiheneinbaugeräte im Verteiler

Welche Daten wurden zu welchem Zeitpunkt über die DSS ausgetauscht?

Zur Kundenanlage: Hüllkurven präventiv und kurativ für Verbrauch und Einspeisung, Leistung = 0 W entspricht dabei einem Schaltsignal direkt auf die Relaiskontakte.

Gab es eine Quittierung seitens der Netzkunden?

Ja, vom gridoo Brain in Form übermittelter Messwerte (Leistung in Echtzeit)

In welcher Granularität wurden Daten ausgetauscht?

Ja, zum dataHub beim VNB werden Echtzeitdaten übertragen (Leistung, aber auch andere Daten vom Smart Meter wären verfügbar). Latenzzeit < 3 Sekunden

Wurden Anforderungen an Cybersecurity betrachtet und welche Art der Authentifizierung gab es?

End-to-End verschlüsselt auf Basis TLS. Architektur berücksichtigt Anforderungen aus dem BDEW-Whitepaper. Jedes gridoo Brain ist ab Werk mit einem vom Betreiber digital signierten, individuellen Zertifikats-Set ausgestattet, das beim Verbindungsaufbau geprüft wird. Zusätzlich enthält das Brain den Public Key des VNB, um eine Authentifizierung des VNB gegenüber dem Brain zu ermöglichen.

Wurden mehrere gegenläufige Steuersignale / Einsatzinformationen getestet? Wenn ja, welche Prioritätsregeln wurden definiert?

Im gridoo Brain werden Lastvorgaben des VNB gegenüber anderen Steuersignalen priorisiert.

Wo findet die Koordinierung der flexiblen Einheiten statt?

Im EMS, also dem gridoo Brain.

Welches Monitoringkonzept wurde berücksichtigt? Wie konnte bspw. sichergestellt werden, dass die von einer flex. Einheit angeforderte netzdienliche Leistung auch am Zählpunkt angekommen ist?

Die aktuellen Leistungswerte des Smart Meters und verfügbarer flexiblen Einheiten könnten vom gridoo Brain in Echtzeit übermittelt werden.

Welches Update-Management ist bei der angestrebten Lösung vorgesehen bzw. denkbar? Sind Funktionserweiterungen möglich? Welche Akteure müssten eingebunden werden?

Ja, Funktionserweiterungen können durch das integrierte Updatemanagement entweder vom Hersteller gridoo oder vom VNB anlagenspezifisch ausgerollt werden. Serverseitig, also im dataHub beim VNB, sind Erweiterungen laufend möglich.

Wie resilient / robust ist die angestrebte Lösung, insb. mit Blick auf den Ausfall kritischer Infrastruktur bzw. wichtiger Komponenten? Kann ein Teilbetrieb aufrecht erhalten werden (z. B. bei dezentralen Ansätzen)? Welche Rückfallebenen sind in Situationen mit Störungen vorgesehen? Welche Fall-back-Prozesse wurden definiert? Wie anfällig ist das Lösungskonzept mit Blick auf Manipulationen, bspw. mit Blick auf ungewünschtes Netznutzerverhalten?

Das gridoo Brain arbeitet bei Ausfall der Kommunikation zum VNB zeitlich unbegrenzt mit vorab übertragenen Fallback-Leistungskurven. Der Verbindungsstatus (Health State) der Kommunikation wird auf beiden Seiten überwacht, ein Ausfall kann an übergeordnete Stellen (API beim VNB und Smartphone-Notifications beim Kunden) gemeldet werden.

Aus datentechnischer Sicht ist die Lösung vollständig abgesichert, jeder Befehl kann zusätzlich digital signiert werden. Was bleibt, ist die Manipulation in Form von Abklemmen durch den Nutzer.

Mit Blick auf die DSS: Wo werden Standardisierungsnotwendigkeiten gesehen?

Wir sehen die Herausforderung bei der Ausarbeitung des openAdr 3.1 Standardprofils im Spagat zwischen rascher Umsetzung (in die Gänge kommen) und Berücksichtigung zukünftig denkbarer Anwendungen (nicht unnötig einschränken). Als möglichen Ansatz empfehlen wir **die klare Trennung zwischen a) zwingend vorgeschriebenen Funktionen (mandatory) und b) optionalen, noch nicht zwingend final ausformulierten Funktionen**. Dies erscheint auch im Hinblick auf gemeinsam mit dem Regulator abzustimmenden Themen als bevorzugte Herangehensweise.

Welche Herausforderungen sind aufgetreten? Welche Empfehlungen für die Einführung einer DSS leiten Sie aus dem Piloten ab?

Entscheidend für eine erfolgreiche, rasche Einführung sehen wir die **frühzeitige Einbeziehung möglichst aller Stakeholder**. Die beste technische Ausarbeitung nützt nichts, wenn z.B. die regulatorischen Rahmenbedingungen nicht abgestimmt sind.

Ein gemeinsames, aktiv kommuniziertes Bild von breitem Nutzen eines (auch auf den unteren Netzebenen) digitalisierten Stromnetzes wird aus unserer Sicht ein wichtiger Erfolgsfaktor sein. Anders ausgedrückt: Die DSS ist kein notwendiges Übel, sondern eine echte Chance im Sinne eines zukunftssicheren Verteilnetzes.

3.1.3 Pilot 3: Pilot für Energienetze Steiermark

Involvierte Industrieunternehmen: Fronius International GmbH

Laufzeit: 03.04.2025 bis 02.04.2026

Beschreibung des Projektes:

Das Pilotprojekt „Pilot 3a“ involvierte Energienetze Steiermark und Fronius International GmbH mit einer Laufzeit von etwa einem Jahr. Ziel war das Testen der gesamten Prozesskette – von der Installation der Messgeräte bis zur digitalen Schnittstelle und der NIS2-konformen Datenübertragung mittels MQTT-Broker.

Projektziele und Architektur

- Test der gesamten Prozesskette inklusive Einbau von Siemens EGS (enhanced grid sensor) Messgeräten an Abzweigen und Hausanschlüssen sowie Erstellung von Einwilligungserklärungen und Datenschutzinformationen
- Aufbau einer digitalen Schnittstelle über die Fronius Flexibility API, eine REST API, die es ermöglicht eine Schnittstelle zur Fronius Solar.Web-Plattform (Herstellercloud) zur Steuerung und Abfrage von PV-Systemen (Wechselrichtern und Batterien) herzustellen, realisiert als Software in der flexiblen Einrichtung des Kunden
- Umsetzung der Datenübertragung NIS2-konform mit MQTT-Broker und Einrichtung der REST API zur Anbindung der DSS

Steuerung und Datenaustausch

- Einflussnahme auf Wechselrichter und Speicher bei zwei Kunden:
    - Kunde 1: zwei Wechselrichter und ein Speicher
    - Kunde 2: ein Wechselrichter und ein Speicher

- Steuerung erfolgte auf der Ebene der Gesamtheit der flexiblen Einheiten einer Anlage, wobei aber auch jede flexible Einheit selbst angesteuert werden konnte
- Nachdem der Kunde seine Zustimmung für den Zugriff über die Flexibility API gegeben hat, erfolgt die Quittierung der Steuerbefehle automatisch über die API
- Datenübertragung umfasste zunächst Schaltsignale zur Funktionsprüfung, danach Hüllkurven über mehrere Tage
- Für die Hüllkurventests wurden Wetterprognosen, synthetische Lastprofile, Messdaten der Abzweige und Hausanschlüsse sowie die Daten aus der Fronius FlexAPI herangezogen

Cybersecurity und Monitoring

- Umsetzung der relevanten Maßnahmen im Rahmen des Piloten gemäß NIS2-Vorgaben mit Authentifizierung und Token-Management zwischen Netze Data Hub (interne Energienetze Steiermark Plattform, die zum einen Messwerte sammelt, diese der internen Abteilung zur Hüllkurvenberechnung weitergibt und dann diese Hüllkurven an Fronius Solar.Web weiterschickt) und Fronius Solar.Web
- Kein Test mehrerer gegenläufiger Steuersignale; Prioritätsregeln wurden nicht definiert (kann über die Wechselrichtereinstellungen definiert werden)
- Monitoring erfolgt durch Übertragung und Validierung von Messwerten; ein vollständiges Monitoringkonzept ist noch nicht etabliert
- Update-Management und Resilienzkonzepte aktuell nicht berücksichtigt, da es sich um einen Piloten handelt

Ergebnisse

- Der Prozess verlief insgesamt erfolgreich, und das Ziel – die Schnittstelle zu testen – wurde vollständig erreicht. Die Übergabe der Hüllkurve erfolgte reibungslos über Azure Blob Storage, der im Halb-Stunden-Takt automatisch nach einer neuen Hüllkurve abfragt. Der Schedule wird generiert und einmal täglich an Fronius Solar.Web übermittelt.
- Bei jenem Kunden mit einem Wechselrichter war dieser zeitweise nicht erreichbar (vermutlich aufgrund einer externen Internetstörung). Der Kunde mit zwei Wechselrichtern konnte den Schedule vollständig übernehmen
- Der Testzeitraum war aufgrund der derzeit geringen Globalstrahlung nicht optimal für aussagekräftige Hüllkurventests, da durchgehend eingespeist werden konnte

Fazit/Nächste Schritte

- Umfangreichere Tests dieser Art sind vermutlich erst im Frühjahr/Sommer sinnvoll, wenn die Globalstrahlung wieder erhöht ist
- Nächste Schritte: Anpassung der Lastflussberechnungen und Algorithmen unter Einbeziehung historischer Daten (mindestens 1 Jahr erforderlich)

Schaubild der Kommunikation zwischen den Akteuren:

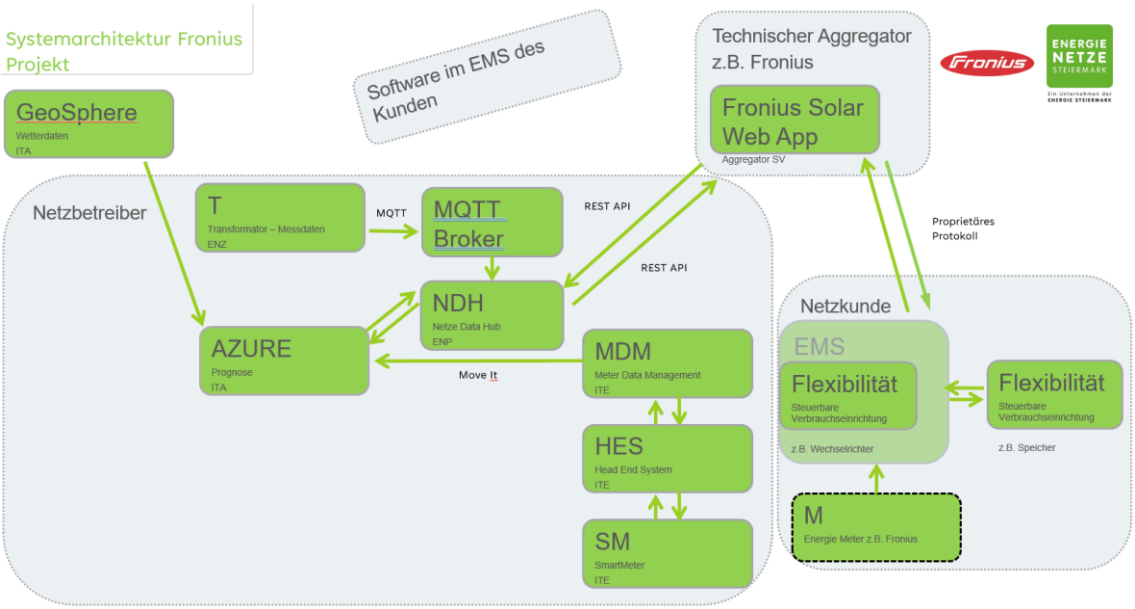


Abbildung 3.3: Schaubild von Pilot 3a

Welche Zielsetzungen wurden verfolgt?

Ziel des Projekts war es, die gesamte Prozesskette umfassend zu testen – beginnend mit dem Einbau der Messgeräte an Abzweigen und Hausanschlüssen bis hin zum Versenden von Steuerbefehlen und anschließende Auswertung. Dazu gehörte auch die Erstellung von Einwilligungserklärungen und Datenschutzinformationen für die Kunden.

Ein weiterer Schwerpunkt lag in der Erarbeitung von Hüllkurven, die auf Basis der Messwerte von Abzweigen und Hausanschlüssen, synthetischen Lastprofilen sowie Wetterprognosen erstellt wurden.

Ein wesentlicher Projektschritt war zudem die Einrichtung einer digitalen Schnittstelle unter Nutzung der Herstellercloud *Fronius Solar.Web über die Fronius Flexibility API*. Darüber hinaus wurde die gesamte Datenübertragung NIS2-konform umgesetzt, wozu auch die Einrichtung eines MQTT-Brokers zur gesicherten Übertragung der Messwerte zählte.

Welche Architekturvariante in der Schnittstelle zum Kunden wurde umgesetzt?

Umgesetzt wurde die Variante Software im EMS des Kunden. Das EMS im Wechselrichter empfängt den Steuerbefehl der Digitalen Schnittstelle über die Flexibility API und steuert den Energiefluss, damit die Leistungsvorgaben in Einspeiserichtung eingehalten werden. Bei angeschlossenem Batteriespeicher steuert es auch dessen Be- bzw. Entladung.

Auf welche flexiblen Einheiten wurde Einfluss genommen?

Es wurde auf Wechselrichter und Batteriespeicher eingewirkt. Insgesamt nahmen zwei Kundenanlagen am Piloten teil, wobei eine Anlage aus zwei Wechselrichtern und einem Speicher bestand und die andere aus einem Wechselrichter und einem Speicher.

In welcher Form wurden die flexiblen Einheiten angesteuert?

Die Ansteuerung erfolgte auf Ebene der Gesamtheit der flexiblen Einheiten (Vorgabe von Einspeiselimits am Netzanschlusspunkt), wobei aber auch jede flexible Einheit selbst angesteuert werden konnte (Steuerbefehle für Wechselrichter bzw. Batterie).

Über welches Kommunikationsmedium wurde die DSS angebunden?

REST API

Wie wurde die DSS beim Kunden installiert?

Im Rahmen des Projekts wurde die DSS als Verbindung online zwischen dem **Netze Data Hub** und der Plattform **Fronius Solar.Web** eingerichtet. Die Umsetzung war vergleichsweise einfach, da die Installation über die Ferne erfolgte. Es war lediglich erforderlich, die Verbindung zwischen dem Netze Data Hub und Fronius Solar.Web online herzustellen. Die Kunden mussten dazu im Solar.Web die Steuerung durch die Energienetze Steiermark freigeben. Dadurch konnte die DSS vollständig eingerichtet werden – ohne Vor-Ort-Termine und ohne den Einbau zusätzlicher Hardware.

Welche Daten wurden zu welchem Zeitpunkt über die DSS ausgetauscht?

Zu Beginn wurde ein einzelnes Schaltsignal übertragen, um die grundsätzliche Funktionsfähigkeit der Schnittstelle zu prüfen. In einem zweiten Schritt erfolgte die Übertragung von **Hüllkurven** über mehrere Tage. Diese Hüllkurven wurden **präventiv**, also im Voraus auf Basis von Prognosedaten, bereitgestellt.

Es wurden nachfolgende Daten ausgetauscht:

Steuerbefehle	Abfragen	Echtzeitdaten
▪ Leistungsvorgabe in Einspeiserichtung am Netzanschlusspunkt ▪ AC-Erzeugungslimit des Wechselrichters ▪ Ladeleistung der Batterie ▪ Entladeleistung der Batterie ▪ Stornierung eines Steuerbefehls	▪ Fahrplan inkl. Status ▪ 5 min Mittelwert Energieproduktion ▪ Metadaten	▪ Status ▪ Einspeiseleistung ▪ Erzeugungsleistung PV ▪ Lade- und Entladeleistung Batterie ▪ SOC Batterie ▪ PowerLoad ▪ PowerOhmpilot ▪ PowerOutput ▪ RateSelfConsumption ▪ RateSelfSufficiency

Tabelle 3.1: Ausgetauschte Daten

Gab es eine Quittierung seitens der Netzkunden?

Nachdem der Kunde seine Zustimmung für den Zugriff über die Flexibility API gegeben hat, erfolgt die Quittierung der Steuerbefehle automatisch über die API. Über die Flexibility API ist die Quittierung der Befehle einsehbar.

In welcher Granularität wurden Daten ausgetauscht?

Im Rahmen des Projekts wurden mehrere Testfälle durchgeführt:

- Testfall 1: Längere Ansteuerung über mindestens 10 Minuten über einen erweiterten Zeitraum zur Überprüfung des stabilen Betriebs
- Testfall 2: Danach Hüllkurventests über mehrere Tage

Die Tests zeigen, dass die Daten in kurzer Granularität ausgetauscht wurden und die Reaktionen nahezu in Echtzeit erfolgten. Eine definierte Latenzzeit wurde im Rahmen der Testfälle implizit durch die Steuerbefehle vorgegeben.

Die Siemens EGS-Messgeräte können Daten im 10 Sekunden Takt senden und messen Spannungen, Ströme und berechnen die Wirk- und Blindleistung sowie den Phasenwinkel.

Weiters erfolgte die Übermittlung von Daten von Fronius Solar.Web:

- Gesamtenergie (Update alle 5 min)
- Echtzeitdaten (Update alle 20 Sek.)

Wurden Anforderungen an Cybersecurity betrachtet und welche Art der Authentifizierung gab es?

Im Rahmen des Projekts wurde der **MQTT-Broker** gemäß den Vorgaben der **NIS2-Richtlinie** eingerichtet.

Cybersecurity: Aus dem Piloten heraus wurden keine Anforderungen an die Cybersecurity gestellt. Fronius stellt jedoch generelle Anforderungen an die Sicherheit der API und somit erfüllt sie gültige Sicherheitsvorgaben (NIS2, regelmäßige Pen-Tests, ISO 27001, europäische Server, OWASP-Kriterien, CRA; EN 303645)

Authentifizierung: Über einen automatisierten Vorgang authentifiziert sich der Kunde/der Verteilernetzbetreiber für den Kunden initial über E-Mail Adresse und Seriennummer. Diese Daten werden dann an Fronius übermittelt und ein Opt-in E-Mail an den Kunden geschickt. Nach erfolgreichen Opt-in (Kunde gewährt VNB den Zugriff auf sein PV-System, erhält der VNB den Steuerzugriff und somit die Global Unique ID (GUID).

Wurden mehrere gegenläufige Steuersignale / Einsatzinformationen getestet? Wenn ja, welche Prioritätsregeln wurden definiert?

Nein

Wo findet die Koordinierung der flexiblen Einheiten statt?

Die Koordinierung der flexiblen Einheiten (Wechselrichter und Speicher) erfolgt über das im Wechselrichter integrierte EMS.

Welches Monitoringkonzept wurde berücksichtigt? Wie konnte bspw. sichergestellt werden, dass die von einer flex. Einheit angeforderte netzdienliche Leistung auch am Zählpunkt angekommen ist?

Derzeit werden Messwerte übertragen und validiert, um die Umsetzung der angeforderten netzdienlichen Leistung zu überprüfen. Durch Abfrage der Einspeiseleistung über die Flexibility API kann sichergestellt werden, dass die von der flex. Einheit angefordert netzdienliche Leistung am Zählpunkt umgesetzt wurde. Ein vollständiges, umfassendes Monitoringkonzept ist jedoch bislang noch nicht eingerichtet und soll zu einem späteren Zeitpunkt entwickelt werden.

Welches Update-Management ist bei der angestrebten Lösung vorgesehen bzw. denkbar? Sind Funktionserweiterungen möglich? Welche Akteure müssten eingebunden werden?

Da es sich derzeit um einen **Piloten** handelt, wurde ein Update-Management bislang nicht berücksichtigt. Updatemanagement und Funktionserweiterungen sind in Absprache zwischen VNB und Hersteller (konkret für diesen Piloten Energienetze Steiermark und Fronius) möglich. Das Updatemanagement könnte zukünftig auch über ein SLA geregelt werden. Je nachdem, wie sich die Entwicklung der digitalen Schnittstelle österreichweit gestaltet, werden mögliche Funktionserweiterungen von den Ergebnissen des Pilotprojekts abhängig gemacht und in Abstimmung mit den beteiligten Herstellern geplant.

Wie resilient / robust ist die angestrebte Lösung, insb. mit Blick auf den Ausfall kritischer Infrastruktur bzw. wichtiger Komponenten? Kann ein Teilbetrieb aufrecht erhalten werden (z. B. bei dezentralen Ansätzen)? Welche Rückfallebenen sind in Situationen mit Störungen vorgesehen? Welche Fall-back-Prozesse wurden definiert? Wie anfällig ist das Lösungskonzept mit Blick auf Manipulationen, bspw. mit Blick auf ungewünschtes Netznutzerverhalten?

Da es sich derzeit um einen **Piloten** handelt, wurden spezifische Konzepte zur Resilienz und Robustheit – etwa für den Ausfall kritischer Infrastruktur oder wichtiger Komponenten – bislang nicht umgesetzt.

Das Lösungskonzept wurde bisher nicht systematisch auf Anfälligkeit gegenüber Manipulationen oder ungewünschtem Nutzerverhalten geprüft.

Für einen späteren Rollout müssten diese Aspekte – insbesondere die Sicherstellung des Betriebs ohne direkten Zugriff des Netzbetreibers – gemeinsam mit den Herstellern und Technologiepartnern entwickelt und getestet werden, insbesondere falls weiterhin auf die Hersteller-Cloud gesetzt wird.

Der Default-Wert muss mit jedem Command mitgeschickt werden (Fahrplan). Ein Fail-Safe-Verhalten ist in der verwendeten Lösung vorhanden. Der letzte übermittelte Wert/Control wird verwendet.

Grundsätzlich sind Erweiterungen für Fallback Szenarien (ähnlich zu IEEE 2030.5) implementierbar z.B. setzen eines Defaultwerts.

Teilbetrieb: war im Pilotprojekt kein Thema, kann jedoch in Absprache mit dem Hersteller umgesetzt werden.

Autonome, netzdienliche Funktionen des Wechselrichters (z.B. P(f), Q(U), Q(P), cos(ϕ) (P), …) bleiben aufrecht.

Kombinierbar mit dig. I/Os („Notaus-Schalter“)

Mit Blick auf die DSS: Wo werden Standardisierungsnotwendigkeiten gesehen?

Beim Protokoll zwischen Netzbetreiber und Netznutzer und den zu übermittelnden Daten. Gegebenenfalls sollen auch die Architekturvarianten österreichweit einheitlich umgesetzt werden und es soll zu einer einheitlichen Definition von dynamischer Regelung kommen – z.B. was bedeutet dynamisch, ist auch schon eine saisonale Steuerung zum Beispiel dynamisch.

Welche Herausforderungen sind aufgetreten? Welche Empfehlungen für die Einführung einer DSS leiten Sie aus dem Piloten ab?

Da für die Umsetzung des Piloten nur wenig Zeit zur Verfügung stand, konnten weder das Protokoll IEEE 2030.5 noch das Protokoll OpenADR 3.1 getestet werden. Daher wurde der gesamte Prozess über die Hersteller-Cloud mittels API abgewickelt. Ein Test von IEEE 2030.5 nach Abschluss dieses Piloten war von Beginn des Piloten angedacht. Künftige zentrale Herausforderungen sind die vollständige Vereinheitlichung, Implementierung und Erprobung dieser Kommunikationsprotokolle, eine stabile Echtzeitdatenübertragung der Messwerte aus den Siemens EGS-Geräten, die Integration unterschiedlicher Gerätetypen sowie die Koordination von IT-Sicherheit, Datenschutz und Herstelleranforderungen und die Zusammenführung der Daten, Auswertung und Ableitung von Steuerungshandlungen.

Für die Einführung einer digitalen Schnittstelle (DSS) sollten offene, standardisierte Protokolle, die bereits breite Anwendung bei den flexiblen Einrichtungen finden, österreichweit (bevorzugt

europaweit) einheitlich frühzeitig integriert und mit allen relevanten Herstellern abgestimmt werden.

Die einheitliche österreichische Lösung sollte dann auch europaweit ausgerollt werden.

Die Verwendung von Herstellerclouds, bei angemessener Vergütung, ist aufgrund der kurzen Umsetzungsdauer empfohlen. Im Falle einer Umsetzung ohne Vergütung für die Hersteller wird eine zentrale, österreichweit einheitliche Stelle eingerichtet werden, auf die alle flexiblen Einheiten zugreifen bzw. von der sie die Steuerbefehle erhalten. Bei dieser Lösung muss gewährleistet sein, dass die flexiblen Einheiten weiterhin über andere WAN-Kanäle kommunizieren dürfen. Bei dieser Lösung sei erwähnt, dass das Handling der flexiblen Einheiten ein beträchtlicher Mehraufwand für den Netzbetreiber darstellt.

Notwendig sind zudem ausreichend Zeit für Architekturplanung, Infrastrukturaufbau und Testphasen, ein robustes Störungs- und Monitoringkonzept, klare Datenschutzprozesse sowie eine skalierbare Cloudplattform, um spätere Erweiterungen und den Rollout auf weitere Netzgebiete reibungslos umzusetzen.

Die DSS verursacht sowohl bei den Netzbetreibern als auch den Herstellern **Entwicklungs-, Inbetriebnahme-, Betriebs-, Wartungs-, Instandhaltungs-, Weiterentwicklungs-, Serverinfrastrukturbetriebs- und Lizenzkosten sowie Kosten für die Aufrechterhaltung des Sicherheitsstandards**. Es muss sichergestellt werden, dass sowohl Netzbetreiber als auch Hersteller eine (regulative) Vergütung für die tatsächlich entstehenden, angemessenen Kosten erhalten. Dies muss gesetzlich verankert werden.

3.1.4 Pilot 4: Cloud Gateway für Flexibilitäten für Netz Burgenland

Involvierte Industrieunternehmen: Fronius International GmbH, Burgenland Energie, Hochschule Burgenland mit Projektpartner Scheiber Solutions

Laufzeit: Herbst 2024 bis 2026

Beschreibung des Projektes:

Unser Ansatz eines mögliches DSS Modells umfasst auch die Einbindung möglicher Aggregatoren. Wir möchten ihnen die Steuerungsmöglichkeit über unser Applikation optional anbieten. Es ist unser Bestreben, dass jeder Aggregator bevor er einen Massen-Steuerbefehl absetzt, zuerst bei der zentralen DSS Komponente eine Bestätigung zur Netzverträglichkeit einholt. Zusätzlich liefern wir eine Möglichkeit zur Anbindung diverser flexibler Geräte an die Netzbetreiber, um den Anforderungen des ELWG gerecht zu werden.

Das Cloud Gateway stellt folgende Funktionen zur Verfügung:

- Ermöglichung von systemdienlichen und netzdienlichen Schaltungen für Netzbetreiber (Befehlsausführung inkl. Rückmeldung)
- Ermöglichung von marktdienlichen Schaltungen für Marktakteure (Befehlsausführung inkl. Rückmeldung)
- Überblick von allen im jeweiligen Netzgebiet geplanten und durchgeführten Schaltungen inkl. Veto-Recht für Netzbetreiber
- Eine Einheitliche Schnittstelle zu allen Aggregatoren, um deren Flexibilitäten zu schalten

- Ein Onboarding Prozess für den Kunden, um seine Flexibilitäten zu registrieren und somit zur Verfügung zu stellen - Bezug zu Zählpunkt wird hergestellt
- Eine Plattform zur Entwicklung und Etablierung von Marktmodellen mit Flexibilitäten

Dies wird bewerkstelligt durch folgende Merkmale:

- Eine zentrale Applikation in der Cloud (hochverfügbar) inkl. Schnittstelle wird allen Aggregatoren bereitgestellt, sodass diese Flexibilitäts-Produkte und Dienstleistungen entwickeln können
- Keine zusätzliche Hardware – weder bei Kunden noch bei den Netzbetreibern
- Anbindung von bestehenden Flexibilitäten (z.B.: Wechselrichter, Batterie) – keine zusätzlichen Investitionen des Endkunden notwendig. Die Anbindung unterschiedlichster Flexibilitäten ist bei Projektfortschritt angedacht
- Anbindung der Flexibilitäten durch bestehende Kommunikationsnetze (Internet, LAN, W-LAN). Es ist kein Aufbau einer parallelen Kommunikationsstruktur nötig

Zielbild: Integration des Cloud Gateways bei EDA – EbUtilities und somit eine möglichst einheitliche Lösung für alle Netzbetreiber

Schaubild der Kommunikation zwischen den Akteuren:

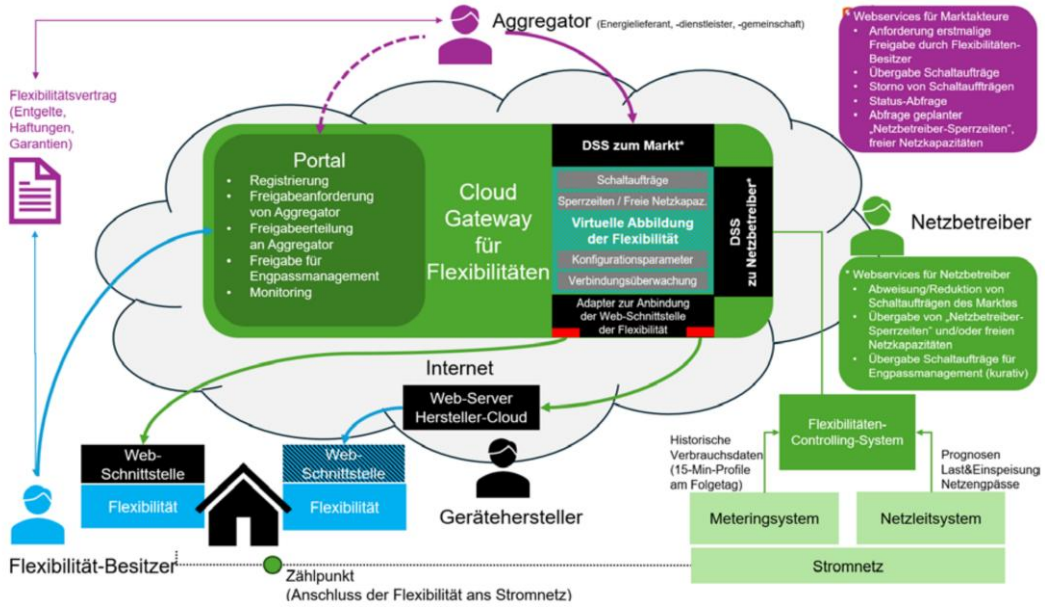


Abbildung 3.4: Schaubild von Pilot Cloud Gateway

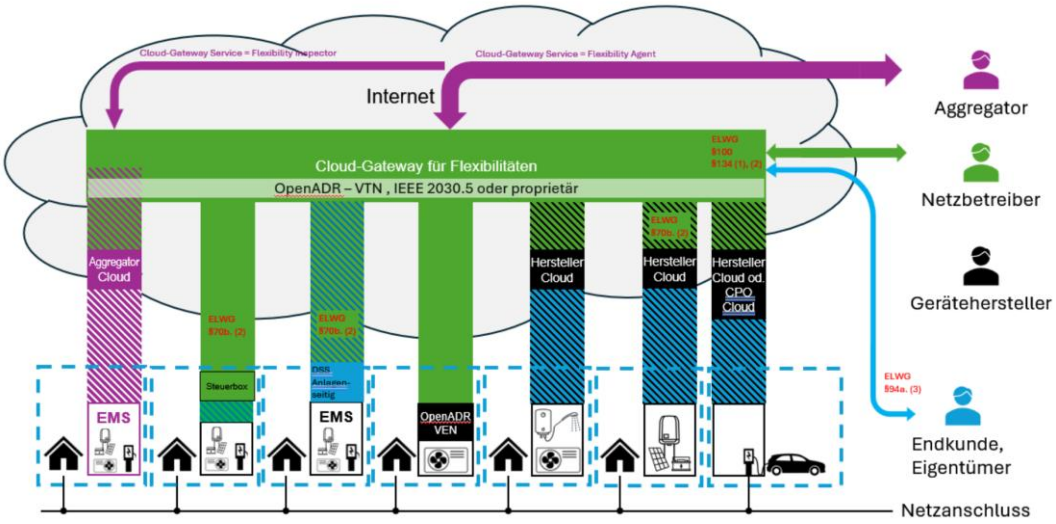


Abbildung 3.5: Architekturübersicht von Pilot Cloud Gateway

Das Architekturübersichtsbild stellt die Ausprägung der diversen Kommunikationskanäle dar.

Die Anbindung der flexiblen Einheiten wurde über die jeweilige Hersteller Cloud durchgeführt. Dies erscheint zweckmäßig für erste Pilot Tests sowie für die Anbindung der Geräte in einer frühen Phase der DSS als Übergangslösung. Spätere Anbindungen über Netzbetreiber eigene Controller ist nicht ausgeschlossen. Zu Projektbeginn war ein Folgeprojekt mit IEEE 2030.5 angedacht. Aufgrund der Empfehlung im Zuge der DSS ist die jeweilige Schnittstelle mit Open ADR 3.1 angedacht. Eine konkrete Festlegung und Ausarbeitung dieser Schnittstelle ist Teil der Weiterentwicklung im Jahr 2026.

Welche Zielsetzungen wurden verfolgt?

Durchführung eines Proof of Concepts inkl. Applikationsentwicklung zur:

- Aufwandsermittlung zur Anbindung von Flexibilitäten über deren Herstellercloud
- Steuerung der Flexilben Einheiten (Wechselrichter und Speicher) über die Fronius Flexiblity API zu testen.
- Sammeln von Erfahrungen zur Verbindungsqualität
- Anbindungsmöglichkeiten an Aggregatoren zu eruieren und zu testen
- Schaltaufträge vor Absenden an die flexible Einheit auf Netzverträglichkeit zu prüfen

Welche Architekturvariante in der Schnittstelle zum Kunden wurde umgesetzt?

Software im EMS des Kunden. Das EMS im Wechselrichter empfängt den Steuerbefehl der Digitalen Schnittstelle über die Flexiblity API und managend den Energiefluss, damit die Leistungsvorgaben in Einspeiserichtung eingehalten werden. Bei angeschlossen Batteriespeicher managet es auch dessen Be- bzw. Entladung.

Auf welche flexiblen Einheiten wurde Einfluss genommen?

Anzahl der flex. Einheiten: 5 / Anzahl Kundenanlagen: 4 / Art: Fronius und Huawei Wechselrichter mit Batterie

Anm.: Huawei (Nicht Teil des offiziellen OE Piloten 4. Außerhalb des Piloten 4 wurde als Erweiterung des Cloud Gateways ebenfalls die Schnittstelle von Huawei integriert)

Ein erster Friendly User Test mit mehreren Anlagen von Energie Burgenland Kunden ist noch ausständig.

In welcher Form wurden die flexiblen Einheiten angesteuert?

Die Ansteuerung erfolgte auf der Ebene der Gesamtheit der flexiblen Einheiten (Vorgabe von Einspeiselimits am Netzverknüpfungspunkt), wobei aber auch jede flexible Einheit selbst angesteuert werden konnte (Steuerbefehle für Wechselrichter bzw. Batterie).

Für den Fall, dass beim Kunden Flexibilitäten unterschiedlicher Hersteller verbaut sind und diese auch über die DSS angesteuert werden sollen, müssen in der jetzigen Konfiguration des Cloud Gateways die flexiblen Einheiten unabhängig voneinander angesteuert werden. Eine diesbezügliche Logik ist in der zentralen Komponente des Cloud Gateways einfach umzusetzen.

Sollte später festgelegt werden, dass für diesen Fall von mehreren unterschiedlichen flexiblen Einheiten unterschiedlicher Hersteller vor Ort eine Hardware der Netzbetreiber eingebaut werden muss, so ist das Cloud Gateway flexibel genug eine Schnittstelle mit Open ADR 3.1 für diese Fälle einzubauen.

Über welches Kommunikationsmedium wurde die DSS angebunden?

Die Ansteuerung ausgehend von der zentralen Komponente (Cloud Gateway Applikation) erfolgt über Netzwerk bzw. Internet zur Cloud Applikation der Hersteller. Dabei wird eine REST API angesprochen. Die Verbindung von der Hersteller Cloud Applikation zur flexiblen Einheit erfolgt über ein IEEE 2030.5 ähnliches proprietäres Protokoll.

Im Zuge der Weiterentwicklung bzw. Spezifizierung der DSS soll das Kommunikationsprotokoll auf Open ADR 3.1 umgestellt werden

Wie wurde die DSS beim Kunden installiert?

Ein wesentlicher Vorteil dieses Konzepts ist es, dass keine Hard- oder Software beim Kunden installiert werden muss.

Die Verbindung wurde online zwischen den Systemen der Netz Burgenland und Fronius Solar.Web eingerichtet. Die Umsetzung war vergleichsweise einfach, da die Installation über die Ferne erfolgte. Es musste lediglich online die Verbindung zwischen Cloud Gatewayund Fronius Solar.Web hergestellt werden und die Kunden musste die Steuerung durch Netz Burgenland online im Solar.web freigeben. Somit konnte die DSS ohne Anfahrten und Einbau zusätzlicher Hardware hergestellt werden.

Welche Daten wurden zu welchem Zeitpunkt über die DSS ausgetauscht?

Aktuell werden in der Applikation folgende Schaltbefehle zur Steuerung von Wechselrichtern der Marke Fronius und Huawei durchgeführt.

- Kurativ: Energie in den Speicher laden; Energie aus dem Speicher ins Netz entladen;(fixer Leistungswert oder als Hüllkurve)
- Präventiv: Exportlimit setzen (Hüllkurve)

Die Hüllkurven lassen sich mit einem bereits implementierten Schedular (Fahrplan) umsetzen.

Die Auslesung von Daten aus den flexiblen Assets beschränkt sich aktuell auf Stammdaten der Assets sowie einer zyklischen (alle 5 Minuten) Auslesung des State of Charge der Speicher. Dadurch lässt sich auch die Verbindungsqualität aufzeichnen.

Die Auslesung weiterer Daten lässt sich sehr einfach umsetzen. Die Hersteller verfügen über einen hohen Detailgrad von Energiedaten und stellen diese über deren Cloud Applikation bereit.

Z.B.:

- Fahrplan inkl. Status
- 5 min Mittelwert Energieproduktion
- Metadaten
- Status
- Einspeiseleistung
- Erzeugungsleistung PV
- Lade- und Entladeleistung Batterie

Gab es eine Quittierung seitens der Netzkunden?

Nachdem der Kunde seine Zustimmung für den Zugriff über die Flexiblity API geben hat, erfolgt die Quittierung der Steuerbefehle automatisch über die API.

Der Kunde muss in der Applikation auch separat zur Steuerung seiner Geräte durch den Aggregator zustimmen.

In welcher Granularität wurden Daten ausgetauscht?

Aktuell nur initiale Stammdaten und State of Charge alle 5 Minuten – u.a. zur Kommunikationsüberwachung.

Es wurde aktuell noch von einer Übermittlung von weiteren Daten abgesehen. Dies lässt sich jedoch sehr einfach erweitern. Z.B. Gesamtenergie (Update alle 5 min)

Echtzeitdaten (Update alle 20 Sek.)

Es wurden aktuell noch keine Use-Cases im Proof of Concept behandelt bei denen weitere Daten außer dem SOC relevant sind. Dies ist jedoch für Weiterentwicklungen vorgesehen.

Wurden Anforderungen an Cybersecurity betrachtet und welche Art der Authentifizierung gab es?

In der momentanen Proof of Concept Applikation verwenden wir die AWS Cloud. Die Verbindungen zwischen den Applikationen sind nach Stand der Technik abgesichert (TLS sowie Shared Secret und Web Token.

Aus dem Piloten heraus wurden keine Anforderungen an die Cybersecurity gestellt. Fronius stellt jedoch generelle Anforderungen an die Sicherheit der API und somit erfüllt sie gültige Sicherheitsvorgaben (NIS2, regelmäßige Pen-Tests, ISO 27001, europäische Server, OWASP-Kriterien, CRA; EN 303645)

Authentifizierung:

Steuerung zwischen Cloud Gateway und Fronius Solar.Web

Über einen automatisierten Vorgang authentifiziert sich der Kunde bzw. Cloud Gateway für den Kunden initial mit E-Mail Adresse und Seriennummer des Wechselrichters. Diese Daten werden dann an Fronius übermittelt und ein Opt-in E-Mail an Kunden geschickt. Nach erfolgreichen Opt-in (Kunde gewährt VBN den Zugriff auf sein PV-System) erhält der VNB den Steuerzugriff und somit die Global unique ID (GUID).

Steuerung zwischen Aggregator und Cloud Gateway

Das Cloud Gateway arbeitet im Hintergrund mit der Kunden-Datenbank von Netz Burgenland. Der Kunde loggt sich mit seinem Account ein uns ist somit authentifiziert.

Um Steuerbefehle von Aggregatoren dem Kunden bzw. auf die Anlage zuweisen zu können wurden diese Befehle auf Zählpunktbasis aufgebaut. Ein Kunde gibt vorab die Zustimmung zur Steuerung seiner flex. Einrichtungen durch den Aggregator in der Applikation. Hierbei wurde ein Token verwendet.

Wurden mehrere gegenläufige Steuersignale / Einsatzinformationen getestet? Wenn ja, welche Prioritätsregeln wurden definiert?

Die Einstellungen des Wechselrichters bestimmen die Priorisierung der Befehle von dessen unterschiedlichen Interfaces

Nein, im Piloten wurden noch keine gegenläufige Steuersignale getestet. Es ist anzumerken, dass in jeder anderen Architektur die Priorisierung ebenfalls vom Hersteller behandelt werden muss.

Wo findet die Koordinierung der flexiblen Einheiten statt?

Die Koordinierung der flexiblen Einheiten (Wechselrichter und Speicher) erfolgt über das im Wechselrichter integrierte EMS.

Eine darüberhinausgehende Koordinierung von mehreren flexiblen Einheiten in der Anlage wurde noch nicht umgesetzt.

Welches Monitoringkonzept wurde berücksichtigt? Wie konnte bspw. sichergestellt werden, dass die von einer flex. Einheit angeforderte netzdienliche Leistung auch am Zählpunkt angekommen ist?

Aktuell wird nur der SoC alle 5 Minuten ausgelesen. Daraus lassen sich für netzdienliche Schaltungen Schlüsse ziehen. Ebenfalls wird diese Anzeige zur Verbindungsüberwachung verwendet.

Durch eine leicht umzusetzende Abfrage der Einspeiseleistung oder anderer Daten über die solar.web Flexibility API kann sichergestellt werden, dass die von der flex. Einheit angefordert netzdienliche Leistung am Zählpunkt umgesetzt wurde.

Welches Update-Management ist bei der angestrebten Lösung vorgesehen bzw. denkbar?

Updates an der zentralen Komponente des Cloud Gateways sind allein durch die Netzbetreiber bzw. deren Entwicklungspartner durchführbar.

Updates von den dezentralen Komponenten werden von den Herstellern durchgeführt. Die Updatemöglichkeit ist bei vielen Geräten gegeben. Ein notwendiges Update muss mit dem Hersteller der Flexibilität koordiniert werden. Hierzu ist ein SLA ratsam.

Sind Funktionserweiterungen möglich? Welche Akteure müssten hierbei eingebunden werden?

Ein wesentlicher Vorteil unseres Konzepts ist es, dass Funktionserweiterungen sehr einfach umzusetzen sind. Sehr viele bereits geforderte oder auch neue Funktionen lassen sich rein zentral in der Applikation Cloud Gateway abbilden. Hierzu müssen nur die Netzbetreiber bzw. die Betreiber der zentralen DSS Komponente eingebunden werden. Dies führt zu einer erheblichen Beschleunigung des Rollouts. Neue Funktionen, die den Funktionsumfang der flexiblen Einheit bzw. die Hersteller API betreffen müssen mit den Herstellern abgestimmt werden.

Wie resilient / robust ist die angestrebte Lösung, insb. mit Blick auf den Ausfall kritischer Infrastruktur bzw. wichtiger Komponenten? Kann ein Teilbetrieb aufrecht erhalten werden (z. B. bei dezentralen Ansätzen)? Welche Rückfallebenen sind in Situationen mit Störungen vorgesehen? Welche Fall-back-Prozesse wurden definiert? Wie anfällig ist das Lösungskonzept mit Blick auf Manipulationen, bspw. mit Blick auf ungewünschtes Netznutzerverhalten?

Es gibt die Möglichkeit, ein Failsafe-Verhalten bei Versand eines Fahrplans vorzugeben. Der Default-Wert für einen späteren Zeitpunkt, bei dem möglicherweise die Verbindung abgebrochen sein wird, muss mit jedem Command mitgeschickt werden (Fahrplan) (Control mit Einspeiselimit am Ende des Fahrplans mit unbestimmter/langer Zeit Dauer).

Grundsätzlich sind Erweiterungen für Fallback Szenarien (ähnlich zu IEEE 2030.5) implementierbar. Z.B. setzen eines Defaultwerts.

Zusätzlich:

- Autonome, netzdienliche Funktionen des Wechselrichters bleiben aufrecht (z.B. P(f), Q(U), Q(P), cos(ϕ)(P), …)
- Kombinierbar mit dig. I/Os („Notaus-Schalter“)

Mit Blick auf die DSS: Wo werden Standardisierungsnotwendigkeiten gesehen?

Beim Protokoll zwischen Netzbetreiber und Netznutzer und den zu übermittelenden Daten.

Eine Konsolidierung der zu verwendenden Stammdaten und Prozesse beschleunigt den Spezifikationsvorgang.

Welche Herausforderungen sind aufgetreten?

Unterschiedliche Adapter mussten spezifiziert und entwickelt werden. Zusätzlich gab es bei jeden Adapter Eigenheiten in der Anbindung auf die man Rücksicht nehmen mussten. Jeder Adapter erfordert separaten Wartungsaufwand Bsp: Bugfindung und Behebung.

Die Anbindung über die Cloud hat jedoch erstaunlich schnell und gut funktioniert.

Unser Konzept beinhaltet auch eine Schnittstelle Flexibilitätsmarkt. In unserem Projekt ist es auch geplant Aggregatoren die Testmöglichkeit auf unserer Applikation zu geben. Die diesbezügliche Abstimmung mit möglichen Aggregatoren war notwendig.

Bis sich Aggregatoren gefunden haben, die unsere Applikation testen, hat es länger gedauert als ursprünglich gedacht. Wir haben nun 1-2 Aggregatoren die bereits jetzt bzw. in absehbarer Zeit die Aggregator Schnittstelle des Cloud Gateways testen.

Es ist geplant Schaltbefehle von Aggregatoren vor deren Durchführung auf Netzverträglichkeit zu bewerten und automatisierte rasche Rückmeldungen an die Aggregatoren zu liefern - damit keine Netzengpässe durch diese Schaltungen ausgelöst werden. Ein Forecast für die Auslastung der Trafostationen auf Basis historischer Daten soll als Grundlage dienen. Es gibt bereits Ansätze für diesen Funktionsbaustein, jedoch wurde er noch nicht genauer spezifiziert oder entwickelt.

Es ist ebenfalls eine Herausforderung Aggregatoren dazu zu bringen, dass sie das Cloud Gateway verwenden und dabei die Hürden für Aggregatoren so gering wie möglich zu halten. Aktuell besteht keine Pflicht für Aggregatoren sich einer DSS anzuschließen.

Welche Empfehlungen für die Einführung einer DSS leiten Sie aus dem Piloten ab?

Wir empfehlen so wenig Hardware wie nur unbedingt notwendig bei den Kunden zu verbauen. Bei einem „Standard“ Haushalt z.B. mit Wechselrichter + Speicher sowie mit Ladesäule und Wärmepumpe sollte keine Hardware oder Software vom Netzbetreiber verbaut oder gewartet

werden müssen. Zukünftig sollen diese Geräte über eine harmonisierte Schnittstelle (Open ADR) über den Internetzugang des Kunden angesprochen werden.

Die DSS sollte auf offene, standardisierte Protokolle, die bereits breite Anwendung bei den flexiblen Einrichtungen finden, österreichweit (bevorzugt europaweit) einheitlich umsetzen und mit allen relevanten Herstellern abgestimmt werden. Die einheitliche österreichische Lösung sollte dann auch europaweit ausgerollt werden.

Im Falle einer Umsetzung ohne Vergütung für die Hersteller wird eine zentrale, österreichweit Einheitliche Stelle eingerichtet werden, auf die alle flexiblen Einheiten zugreifen bzw. von der sie die Steuerbefehle erhalten. Bei dieser Lösung muss gewährleistet sein, dass die flexiblen Einheiten weiterhin über andere WAN-Kanäle kommunizieren dürfen. Bei dieser Lösung sei erwähnt, dass das Handling der flex. Einheiten ein beträchtlicher Mehraufwand für den Netzbetreiber darstellt.

Die Verwendung von Herstellerclouds, bei angemessener Vergütung, ist aufgrund der kurzen Umsetzungsdauer empfohlen.

Die DSS verursacht sowohl bei den Netzbetreibern als den Herstellern Entwicklungs-, Inbetriebnahme-, Betriebs-, Wartungs-, Instandhaltungs-, Weiterentwicklungs-, Serverinfrastrukturbetriebs- und Lizenzkosten sowie Kosten für die Aufrechterhaltung des Sicherheitsstandards. Es muss sichergestellt werden, dass sowohl Netzbetreiber als auch Hersteller eine (regulative) Vergütung für die tatsächlich entstehenden, angemessenen Kosten erhalten. Dies muss gesetzlich verankert werden.

3.1.5 Pilot 5: EnWG §14a für Voralberger Energienetze & e-netze Allgäu

Involvierte Industrieunternehmen: PSI, Prolan, Voltaris, PPC

Laufzeit: 01.01.2024 – 31.12.2026

Beschreibung des Projektes:

Durch die überarbeiteten Regelungen des § 14a EnWG stehen die Verteilernetzbetreiber und Messstellenbetreiber in Deutschland vor großen Herausforderungen. Um die Herausforderungen der Energiewende zu bewältigen, ermöglicht der Gesetzgeber dem Verteilernetzbetreiber neben dem klassischen Netzausbau zusätzlich die Reduzierung der Wirkleistung von Flexibilitäten (Ladestellen, Wärmepumpen, Klimageräte und Batteriespeicher P > 4,2 kW), um bei Netzengpässen die Netze zu entlasten. Im Gegenzug dazu erhält jeder Kunde eine Reduzierung der Netzentgelte. Um die gesetzlichen Fristen zu erfüllen, wurde in einem Projekt für die e-netze allgäu die Anforderungen erarbeitet und Handlungsempfehlungen für die Bereiche Recht, Netzwirtschaft, Netzbetrieb, Messtechnik, Netzplanung und Netzführung ausgearbeitet. Im Projekt wurde dabei ein modulares Konzept für die intelligenten Ortsnetzstationen (iONS) erarbeitet, wodurch die Digitalisierung der Netze optimiert werden kann. Für eine netzdienliche Ansteuerung der Flexibilitäten wurde eine Potenzialanalyse nach Vorgaben § 14a EnWG unter Berücksichtigung der gesetzlichen Rahmenbedingungen durchgeführt. Als Basis für eine Ansteuerung ist ein Netzmonitoring/Netzleitsystem notwendig, das den aktuellen Netzzustand abbilden kann und auf dieser Grundlage die Ansteuerung durchzuführen. Dazu wurden die notwendigen Anforderungen erarbeitet und getestet. Die praktische Ansteuerung der steuerbaren Verbrauchseinrichtungen wurde über die vorgeschriebene Smart Meter Infrastruktur bis zur Kundenanlage analysiert, notwendige Maßnahmen erarbeitet und teilweise erprobt.

Die größten Herausforderungen zur Erfüllung der vollständigen Ansteuerung der steuerbaren Verbrauchseinrichtungen sind folgende Punkte:

- Steuerungsrollout des intelligenten Messsystems + Rollout intelligente Trafostation
- Anpassung ERP-System und Aufbau CLS-Kommunikation zwischen VNB, MSB, GWA und Kunde
- Bereitstellung und Verarbeitung der Smart Meter Daten sowie iONS-Messwerte (Datendrehschreibe)
- Aufbau eines NS-Monitoring/Leitsystem
- Erstellung und Umsetzung erforderliche Prozesse und Workflows innerhalb des VNBs

Schaubild der Kommunikation zwischen den Akteuren:

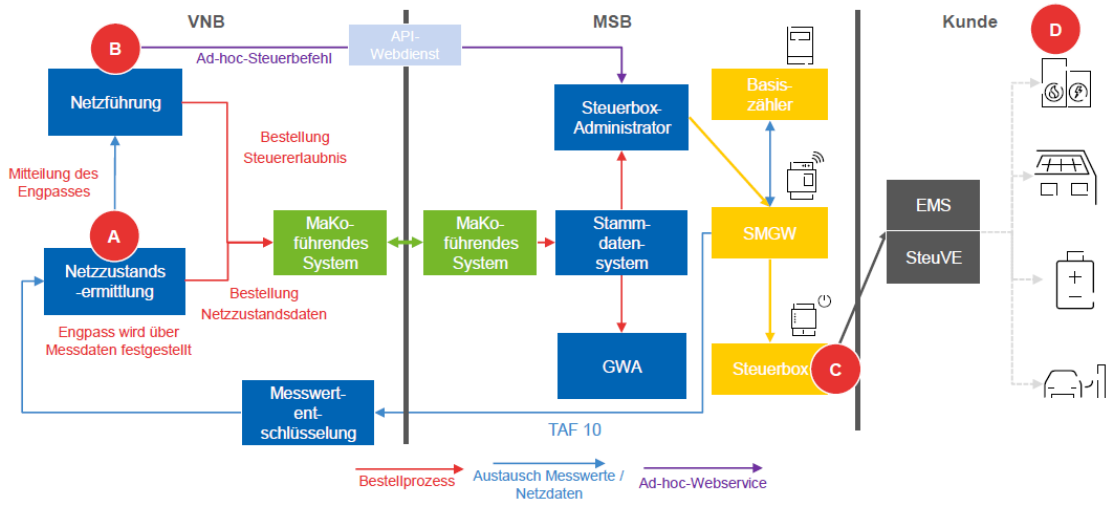


Abbildung 3.6: Architekturbild von Pilot EnWG §14a (Quelle: VDE, FNN)

Welche Zielsetzungen wurden verfolgt?

Erarbeitung der notwendigen Maßnahmen zur Ansteuerung der steuerbaren Verbrauchseinheiten nach EnWG §14a in Deutschland

Welche Architekturvariante in der Schnittstelle zum Kunden wurde umgesetzt?

Steuerbox von Firma Prolan in Kundenanlage, Ansteuerung über Smart Meter Infrastruktur

Auf welche flexiblen Einheiten wurde Einfluss genommen?

PV-Anlagen und Ladeeinrichtung jeweils 1x

In welcher Form wurden die flexiblen Einheiten angesteuert?

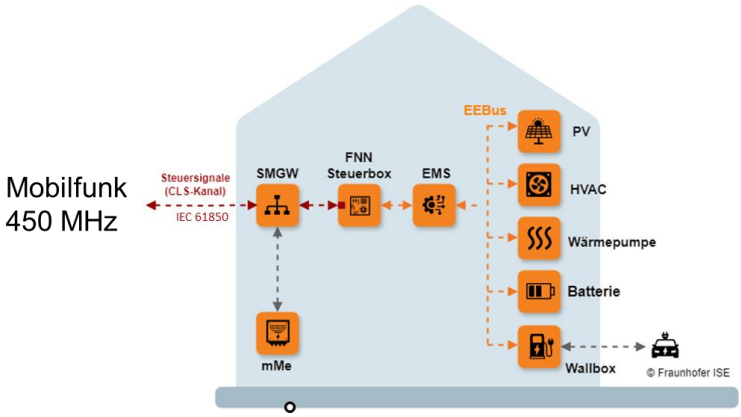
Einzelne flexible Einheit einer Anlage

Über welches Kommunikationsmedium wurde die DSS angebunden?

Mobilfunk

Wie wurde die DSS beim Kunden installiert?

Über Smart Meter Gateway und Steuerbox



Welche Daten wurden zu welchem Zeitpunkt über die DSS ausgetauscht?

Kurative Eingriffe

Gab es eine Quittierung seitens der Netzkunden?

In Deutschland können über verschiedene Tarifanwendungsfälle Informationen und Messwerte abgefragt werden, was den Daten der Digitalen Schnittstelle entspricht. Siehe Tarifstrukturbild:

	NAME	BESCHREIBUNG
TAF 1	Datensparsame Tarife	Auslesen von Zählerstand auch als Summe von Verbrauch und Einspeisung mehrerer Zähler (minimale Auflösung: ein Zählerstand pro Monat).
TAF 2	Zeitvariable Tarife	Zeitabhängiger Stromtarif für mehrere Tarifstufen (ähnlich heutigem HT/NT-System).
TAF 3	Lastvariable Tarife	Leistungsabhängiger Stromtarif für mehrere Laststufen: Die für die jeweilige Stufe zugrunde liegende Leistung kann durch den Istwert oder durch einen Mittelwert bestimmt werden.
TAF 4	Verbrauchsvariable Tarife	Einteilung der verbrauchten Energie in Verbrauchsstufen, wobei jede Stufe ein Mengenkontingent aufweist: Ist das Kontingent einer Stufe überschritten, wird zur nächsthöheren gewechselt.
TAF 5	Ereignisvariable Tarife	Ereignisabhängiger Stromtarif in definierten Tarifstufen: Die Ereignisse können SMGW-intern oder durch einen externen berechtigten Akteur hervorgerufen werden.
TAF 6	Abruf von Messwerten im Bedarfsfall	Für nicht planbare Situationen wie Umzug, Lieferantenwechsel etc. werden für die letzten 6 Wochen tägliche Messwerte vorgehalten.
TAF 7	Zählerstandsgangmessung	Erfassung (im Takt der Registerperiode) und Versendung von Zählerstandsgängen (Verbrauch und Erzeugung).
TAF 8	Erfassung der Extremwerte für Leistung	Min.- bzw. Max.-Leistung im Abrechnungszeitraum wird durch den jeweiligen Leistungsmittelwert je Registereintrag gebildet (Verbrauch und Erzeugung).
TAF 9	Ist-Einspeisung einer Erzeugungsanlage	Leistungsabfrage im Rahmen einer Energiemanagementmaßnahme (darf nicht zu Abrechnungszwecken verwendet werden).
TAF 10	Abruf von Netzzustandsdaten	Periodisch oder bei Ereignis (Über- oder Unterschreitung eines Schwellwertes).
TAF 11	Steuerung von unterbrechbaren Verbrauchseinrichtungen und Erzeugungsanlagen	Bei Steuersignal oder weiteren externen Ereignissen werden der Zeitpunkt sowie der aktuelle Zählerstand festgehalten.
TAF 12	Prepaid-Tarif	Es wird eine bestimme Energiemenge bereitgestellt und bei Überschreiten bzw. einem definierten Schwellwert ein Signal an EMT und Kunde generiert.
TAF 13	Letztverbraucher-Visualisierung	Alternative Bereitstellung der Messwerte an der WAN- anstatt der HAN-Schnittstelle für die Visualisierung.

Tabelle 3.2: Tarifstruktur (Quelle: ffe.de/veroeffentlichungen/messen-und-steuern-ueber-imsys-funktioniert-das/)

In welcher Granularität wurden Daten ausgetauscht?

Die Netzzustandsermittlung muss auf Basis von Echtzeit-Messungen (1-Minute) erfolgen. (Smart Meter Daten + Messungen Trafostation (Trafo+NS-Abgänge). Innerhalb 5 Minuten ab dem Vorliegen des Ereignisses der Netzzustandsermittlung muss die Mitteilung des Netzzustandes und

die automatische Berechnung der Steuerbefehle in der Netzführung, bevor diese mittels API Web Dienst an den MSB erfolgen.

Wurden Anforderungen an Cybersecurity betrachtet und welche Art der Authentifizierung gab es?

Für eine sichere Kommunikation und Steuerung über die Smart Meter Infrastruktur wurde vom Bundesamt für Sicherheit und Informationstechnik (BSI) ein umfangreiches Paket an Richtlinien definiert.

Die technische Richtlinie BSI-TR-03109 beinhaltet die funktionalen Anforderungen, die ein Smart-Meter-Gateway (SMGW) mindestens erfüllen muss. Das Dokument definiert für die Schnittstellen des SMGW detaillierte technische Vorgaben. Darüber hinaus werden interne, logische Abläufe (z.B. die Tarifierung) anhand von Regelwerken, Zusammenspiel zwischen Smart-Meter-Gateway und Sicherheitsmodul (SM) weiter ausgeführt. In der Architektur des intelligenten Messsystems nutzen Produkte einen Kommunikationsadapter nach der TR-03109-5, um eine sichere kommunikative Anbindung von technischen Einrichtungen an das ***Smart-Meter-Gateway*** an dessen Schnittstellen WAN, LMN und HAN zu ermöglichen. Mit dieser Technischen Richtlinie BSI-TR-03109-5 formuliert das BSI Mindestanforderungen an diejenigen Kommunikationsadapter im HAN des SMGW, die eine sichere Anbindung von technischen Einrichtungen an das SMGW über dessen TLS-Proxy-Funktion ermöglichen (CLS-Kommunikationsadapter).

Die technischen Richtlinie BSI-TR-03109-5 beinhaltet die funktionalen und IT-Sicherheitsanforderungen, die CLS-Komponenten mit einem CLS-Kommunikationsadapter mindestens erfüllen müssen. Durch die Umsetzung dieser Anforderungen können sowohl das Vertrauen in die Infrastruktur rund um das intelligente Messsystem gesteigert als auch die Risiken von Angriffen auf diese technischen Einrichtungenverringert werden.

Wurden mehrere gegenläufige Steuersignale / Einsatzinformationen getestet? Wenn ja, welche Prioritätsregeln wurden definiert?

nein

Wo findet die Koordinierung der flexiblen Einheiten statt?

Bisher nur Betrachtung einzelner Komponenten, keine Zusammenfassung mehrere Betriebsmittel. Im FNN VDE ist diese Anwendung aber bereits geregelt. Siehe Schaubild:

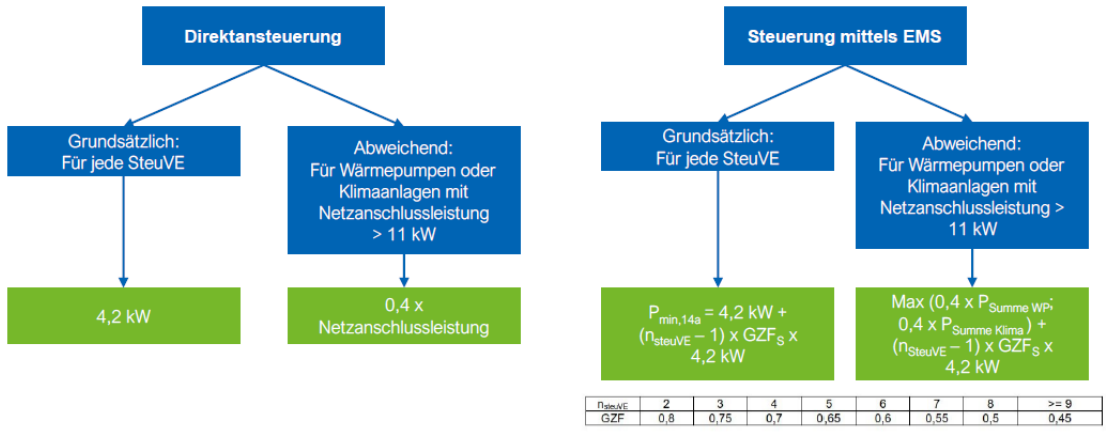


Abbildung 3.7: Koordinierung der Ansteuerung (Quelle: FNN VDE)

Welches Monitoringkonzept wurde berücksichtigt? Wie konnte bspw. sichergestellt werden, dass die von einer flex. Einheit angeforderte netzdienliche Leistung auch am Zählpunkt angekommen ist?

Das Netzmonitoringkonzept basierend auf Messdaten von Trafostation und Smart Meter Daten kann darstellen, ob die Ansteuerung funktioniert hat. Vor der Steuerung wird über den Universabestellprozess sichergestellt, dass die steuerbare Verbrauchseinrichtung auch beim richtigen Kunde platziert und zugeordnet ist und bei der Ad-hoc Steuerung dann richtig funktioniert.

Welches Update-Management ist bei der angestrebten Lösung vorgesehen bzw. denkbar? Sind Funktionserweiterungen möglich? Welche Akteure müssten eingebunden werden?

Updates sind durch die Zertifizierungsrichtlinien möglich und geregelt. Funktionserweiterungen sind möglich (siehe Schaubild zur Erweiterung der Steuerbox). VNB kann im Universalbestellprozess definieren, was bei Ausfall der Kommunikation passieren soll z.B. Mindestwert oder Fahrplan.

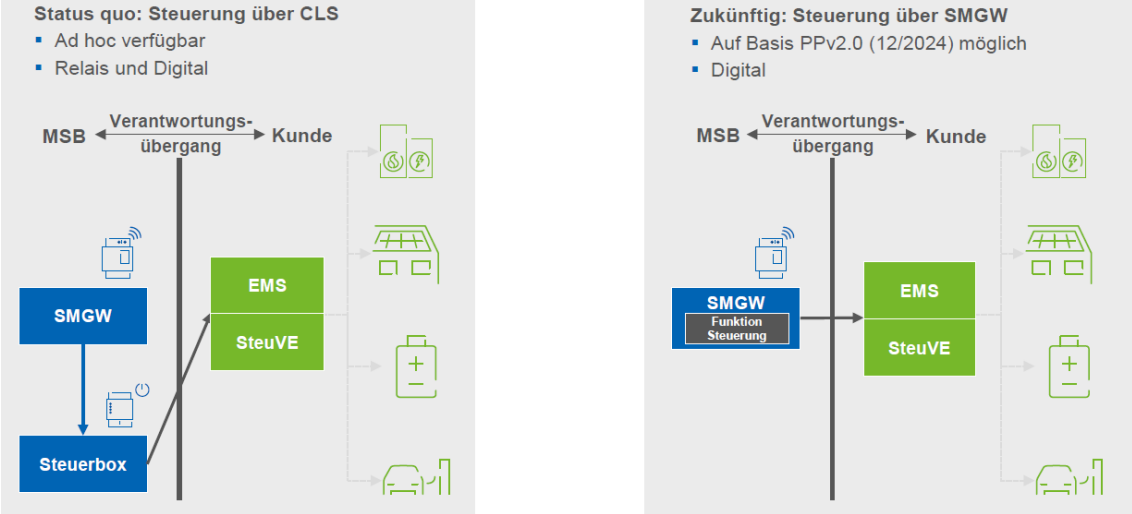


Abbildung 3.8: Erweiterung der Steuerbox (Quelle: FNN VDE)

Wie resilient / robust ist die angestrebte Lösung, insb. mit Blick auf den Ausfall kritischer Infrastruktur bzw. wichtiger Komponenten? Kann ein Teilbetrieb aufrecht erhalten werden (z. B. bei dezentralen Ansätzen)? Welche Rückfallebenen sind in Situationen mit Störungen vorgesehen? Welche Fall-back-Prozesse wurden definiert? Wie anfällig ist das Lösungskonzept mit Blick auf Manipulationen, bspw. mit Blick auf ungewünschtes Netznutzerverhalten?

VNB kann im Universalbestellprozess definieren, was bei Ausfall der Kommunikation passieren soll z.B. Mindestwert oder Fahrplan.

Die Sicherheitsanforderungen gegenüber Manipulation sind aufgrund BSI-Richtlinien sehr hoch und deshalb gut geschützt.

Mit Blick auf die DSS: Wo werden Standardisierungsnotwendigkeiten gesehen?

Hard- und Software zur Erfüllung der DSS Funktionalitäten, Protokolle, Konzept zur Netzzustandsermittlung, Qualität der notwendigen Ansteuerung, Dokumentation der Eingriffe

Welche Herausforderungen sind aufgetreten? Welche Empfehlungen für die Einführung einer DSS leiten Sie aus dem Piloten ab?

Größte Herausforderungen für DE:

- Steuerungsrollout des intelligenten Messsystems + Rollout intelligente Trafostation

- Anpassung ERP-System und Aufbau CLS-Kommunikation zwischen VNB, MSB, GWA und Kunde
- Bereitstellung und Verarbeitung der Smart Meter Daten sowie iONS-Messwerte (Datendrehschreibe)
- Aufbau eines NS-Monitoring/Leitsystem
- Erstellung und Umsetzung erforderliche Prozesse und Workflows innerhalb des VNBs

Empfehlung für DSS AT:

- Technische Entwicklungen und Konzepte für Ansteuerung ermöglichen, keine strikten Vorgaben von Konzepten
- Zertifizierung der Konzepte mit Hard- und Software
- Definition der notwendigen Netzzustandsermittlung für Ansteuerung
- Definition der Qualität der Ansteuerung
- Pflicht für eine Einführung der Ansteuerung im sinnvollen Ausmaß festlegen
- Realistische Ziele für eine Ansteuerung vorgeben, schnelle Echtzeit-Steuerung aufgrund Echtzeit-Messwerte nicht kurzfristig realistisch

3.1.6 Pilot 6: INSIEME für Energienetze Steiermark

Involvierte Industrieunternehmen: EDA, Enfor, Enlite

Laufzeit: 3 Jahre vom 01.04.2025 bis 31.03.2028

Beschreibung des Projektes:

Projektziel

Das EU-Forschungsprojekt INSIEME verfolgt das Ziel, einen gemeinsamen europäischen Energiedatenraum aufzubauen. Dieser ermöglicht den sicheren und standardisierten Austausch von Energiedaten zwischen Netzbetreibern, Kund:innen und Dienstleistern. Damit sollen die Integration erneuerbarer Energien erleichtert, Netzengpässe reduziert und innovative Energiedienstleistungen gefördert werden. Ein zentraler Anwendungsfall ist der flexible Netzanschluss, der die Einspeisung und den Verbrauch dynamisch an die Netzsituation anpasst.

Architektur

Die technische Infrastruktur basiert auf einer Architektur mit direkter Datenanbindung der Kund:innen über den Smart Meter *Österreichs Energie Adapter*. Die Daten werden über die Plattformen **EDDIE** (European Distributed Data Infrastructure for Energy) und **AIIDA** (Admin Interface for In-house Data Access) sicher übertragen. Prognosedienste (ENFOR AS) und Steuerungsalgorithmen (enliteAi GmbH) nutzen diese Daten, um optimale Einspeise- und Lastkorridore zu berechnen.

Steuerung

Im Projekt werden steuerbare Geräte wie PV-Anlagen, Batteriespeicher, Wärmepumpen und E-Ladestationen intelligent geregelt. Die Steuerung erfolgt automatisiert über die digitale Schnittstelle, basierend auf Echtzeit-Messwerten und Lastprognosen. Ziel ist es, Einspeisespitzen zu vermeiden und den Eigenverbrauch zu optimieren.

Cybersecurity
Datensicherheit hat höchste Priorität: Alle Übertragungen erfolgen verschlüsselt und nur mit Einwilligung der Teilnehmer:innen. Zugriff erhalten ausschließlich autorisierte Projektpartner, und personenbezogene Daten werden – soweit möglich – anonymisiert. Internationale Datentransfers erfolgen nur nach DSGVO-konformen Verfahren und mit geeigneten Schutzmaßnahmen.

Monitoring
Das System erfasst kontinuierlich Verbrauchs- und Erzeugungsdaten (z. B. Wirk- und Blindleistung, Ladezustand von Speichern, etc.) in hoher zeitlicher Auflösung. Diese Daten dienen zur Netzstabilitätsanalyse, Optimierung der Steuerungsalgorithmen und Evaluation der Kundenzufriedenheit.

Nächste Schritte

- Kundengewinnung und Installation der notwendigen Hardware (Adapter) bei Teilnehmern
- Anbindung an EDDIE/AIIDA und Inbetriebnahme der Datenübertragung
- Durchführung von Feldtests zur Steuerung flexibler Netzanschlüsse
- Analyse von Netzkapazitätsauslastung, Wirtschaftlichkeit und Akzeptanz

Schaubild der Kommunikation zwischen den Akteuren:

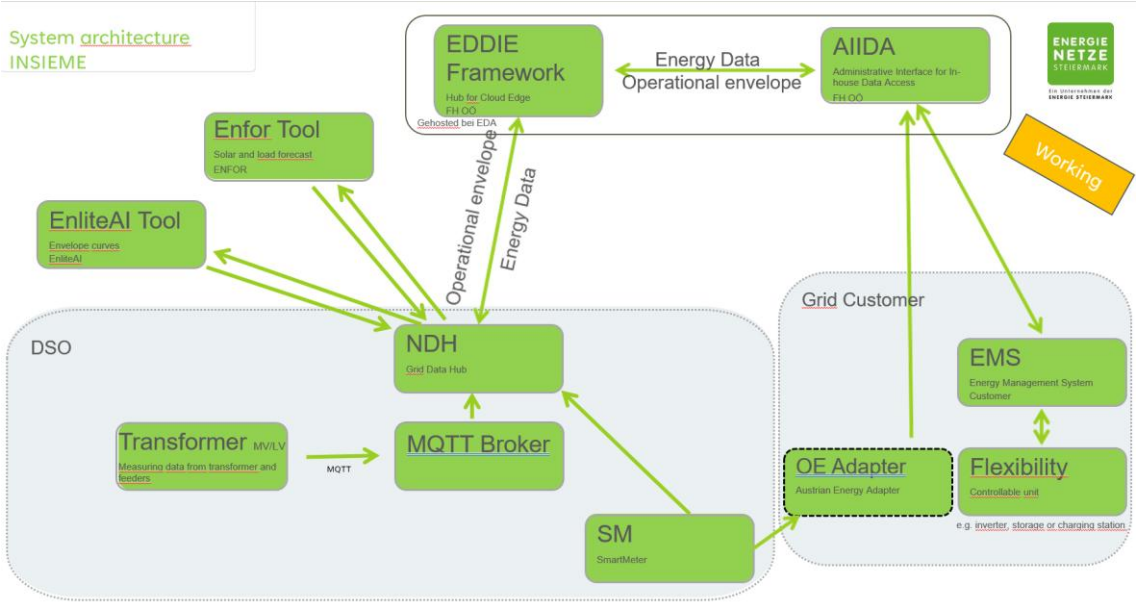


Abbildung 3.9: Schaubild von Pilot Insieme

Welche Zielsetzungen wurden verfolgt?

Test der flexiblen Anschlussvereinbarungen inklusive Integration einer digitalen Schnittstelle zwischen Kunden-EMS und Netzbetreiberplattform

Schwerpunkte:

- Harmonisierung von Datenformaten und Schnittstellen (CIM-Standard)

- Entwicklung von Flexibilitätslösungen mit präventiven Hüllkurven
- Einsatz digitaler Zwillinge zur Erkennung und Simulation von Netzengpässen
- Optimierung von Planungs- und Prognosewerkzeugen für kurz-, mittel- und langfristige Netzplanung
- Hohe Sicherheits- und Datenschutzstandards

Welche Architekturvariante in der Schnittstelle zum Kunden wurde umgesetzt?

Im Projekt soll die Software direkt in der Cloud des EMS des Kunden integriert werden.

Auf welche flexiblen Einheiten wurde Einfluss genommen?

Die Anzahl der teilnehmenden Kund:innen steht derzeit noch nicht fest, aber es soll auf Wechselrichter, Speicher und Ladestationen Einfluss genommen werden.

In welcher Form wurden die flexiblen Einheiten angesteuert?

Die Ansteuerung erfolgt sowohl auf Ebene der gesamten flexiblen Einheiten einer Anlage – beispielsweise durch Vorgabe von Einspeiselimits am Netzanschlusspunkt – als auch gezielt auf einzelne flexible Einheiten.

Über welches Kommunikationsmedium wurde die DSS angebunden?

Die Kommunikation soll über die Cloud mittels CIM basiertem Standard erfolgen.

Wie wurde die DSS beim Kunden installiert?

Im Rahmen des Projekts wird die DSS als Verbindung online zwischen dem **Netze Data Hub** und der EDA Plattform, wo die EDDIE und AIIDA Plattform integriert werden sollen, eingerichtet.

EDDIE (*European Distributed Data Infrastructure for Energy*) bildet eine europaweite, standardisierte Dateninfrastruktur für den Energiebereich. Das Framework konsolidiert Energiedaten aus verschiedenen regionalen oder nationalen Quellen und stellt sie über harmonisierte Schnittstellen und Datenmodelle bereit. Ziel ist die Vereinheitlichung von Zugriffs- und Austauschprozessen, um Interoperabilität zwischen unterschiedlichen Marktakteuren zu gewährleisten und regulatorische sowie technische Fragmentierung zu reduzieren.

AIIDA (*Admin Interface for In-house Data Access*) fungiert als gesicherter, administrativer Zugang zu Mess- und Gerätedaten innerhalb dezentraler Anlagen. Es ermöglicht den direkten, standardisierten und gesicherten Zugriff auf aktuelle Energiedaten aus lokalen Messsystemen (z. B. Smart Meter, Steuergeräte, IoT-Gateways) und überträgt diese in die EDDIE-Infrastruktur. Der Zugriff erfolgt über definierte Berechtigungs- und Authentifizierungsverfahren und kann für verschiedene Anwendungsfälle wie Prognosemodelle, Netzoptimierung oder Energiemanagement genutzt werden.

Welche Daten wurden zu welchem Zeitpunkt über die DSS ausgetauscht?

Geplant: Präventive Übermittlung von Hüllkurven. Details zur Frequenz werden im Projektverlauf festgelegt.

Gab es eine Quittierung seitens der Netzkunden?

Eine Quittierung ist über die AIIDA Plattform vorgesehen, die Details dazu können erst zu einem späteren Zeitpunkt im Projekt genau genannt werden.

In welcher Granularität wurden Daten ausgetauscht?

Dies muss im Projekt erst definiert werden.

Wurden Anforderungen an Cybersecurity betrachtet und welche Art der Authentifizierung gab es?

Zu diesen Themen gibt es eigene Arbeitspakete im Projekt, die gerade erst gestartet haben. Die konkrete technische Umsetzung wird im Projektverlauf definiert.

Wurden mehrere gegenläufige Steuersignale / Einsatzinformationen getestet? Wenn ja, welche Prioritätsregeln wurden definiert?

Derzeit nicht Ziel im Projekt; möglicher Test bei ausreichender Zeit.

Potenzielle Priorität: Netzbetreiber > Aggregator.

Wo findet die Koordinierung der flexiblen Einheiten statt?

Noch offen, wird im Projekt festgelegt.

Welches Monitoringkonzept wurde berücksichtigt? Wie konnte bspw. sichergestellt werden, dass die von einer flex. Einheit angeforderte netzdienliche Leistung auch am Zählpunkt angekommen ist?

Dies muss noch definiert werden.

Welches Update-Management ist bei der angestrebten Lösung vorgesehen bzw. denkbar? Sind Funktionserweiterungen möglich? Welche Akteure müssten eingebunden werden?

Dies muss noch definiert werden.

Wie resilient / robust ist die angestrebte Lösung, insb. mit Blick auf den Ausfall kritischer Infrastruktur bzw. wichtiger Komponenten? Kann ein Teilbetrieb aufrecht erhalten werden (z. B. bei dezentralen Ansätzen)? Welche Rückfallebenen sind in Situationen mit Störungen vorgesehen? Welche Fall-back-Prozesse wurden definiert? Wie anfällig ist das Lösungskonzept mit Blick auf Manipulationen, bspw. mit Blick auf ungewünschtes Netznutzerverhalten?

Darüber kann am Ende des Projektes berichtet werden.

Mit Blick auf die DSS: Wo werden Standardisierungsnotwendigkeiten gesehen?

Protokoll zwischen Netzbetreiber und Netznutzer, einheitliche Definition von Dateninhalten, Harmonisierung Architekturvarianten innerhalb Österreichs/Europas, klare Definition „dynamische Regelung“.

Welche Herausforderungen sind aufgetreten? Welche Empfehlungen für die Einführung einer DSS leiten Sie aus dem Piloten ab?

Nachdem das Projekt noch ziemlich am Beginn ist, kann nur von den bisherigen Herausforderungen berichtet werden. Die Datenschutzthemen sind bei diesem Thema sehr zentral und benötigen auch relativ viel zeitliche Ressourcen. Zusätzlich machen die unterschiedlichen Gegebenheiten in den Ländern es schwierig einheitliche Prozesse (reference Models) zu definieren.

3.1.7 Pilot 7: Projekt EMMA für KNG-Kärnten Netz

Involvierte Industrieunternehmen: Schneider Electric, Emulate

Laufzeit: 2025 – laufend (Pilotbetrieb)

Beschreibung des Projektes:

Im Projekt EMMA (Energiezukunft Modellregion Mittelkärnten und Althofen) wurde eine cloudbasierte Lösung zur netzdienlichen Steuerung von Kundenanlagen erprobt. Die Kommunikation und Steuerung erfolgte über die Plattform Emulate in Kombination mit Messwerten von Schneider Electric. Ziel war es, Betriebsmittel wie Wärmepumpen, Photovoltaikanlagen und Speicher direkt am Netzanschlusspunkt anzusteuern, ohne physische Eingriffe in die Kundeninstallation.

Emulate übernahm eine zentrale Rolle als Aggregator. Über ein benutzerfreundliches Frontend konnten Kunden registriert und steuerbare Lasten sowie PV-Anlagen über Hersteller-APIs eingebunden werden. Die Steuerung basierte auf Hüllkurven, die vom Netzbetreiber bereitgestellt wurden. Für eine zuverlässige Umsetzung war zusätzlich die Integration aktueller Ist-Werte aus dem Netz erforderlich, was die Einbindung von Schneider-Messdaten notwendig machte. Die Vielfalt der Hersteller-APIs erwies sich dabei als komplexe Herausforderung.

Ein physisch getrenntes Netzwerk zwischen Schneider-Geräten und Emulate wurde nicht eingerichtet. Stattdessen übermittelte der Panel Server die Messwerte per LTE an die Schneider-Cloud, von wo Emulate die Daten über eine API abruft. Diese Architektur gewährleistete Netzsicherheit und klare Verantwortlichkeiten, da keine direkte Verbindung zwischen den Systemen bestand.

Auf bestehende Schneider-Lösungen zur Stationsüberwachung wurde bewusst verzichtet, da diese eine Installation spezifischer Hardware in jedem Haushalt erfordert hätten. Der gewählte Ansatz vermeidet Eingriffe in private Kundeninstallationen und ermöglicht eine skalierbare Lösung ohne Vor-Ort-Maßnahmen.

Schaubild der Kommunikation zwischen den Akteuren:

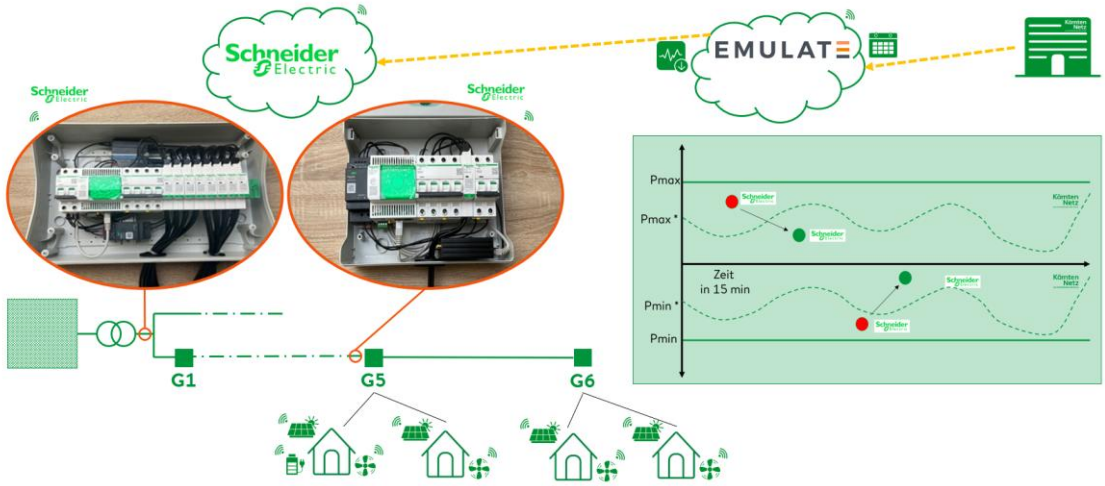


Abbildung 3.10: Schaubild von Pilot EMMA

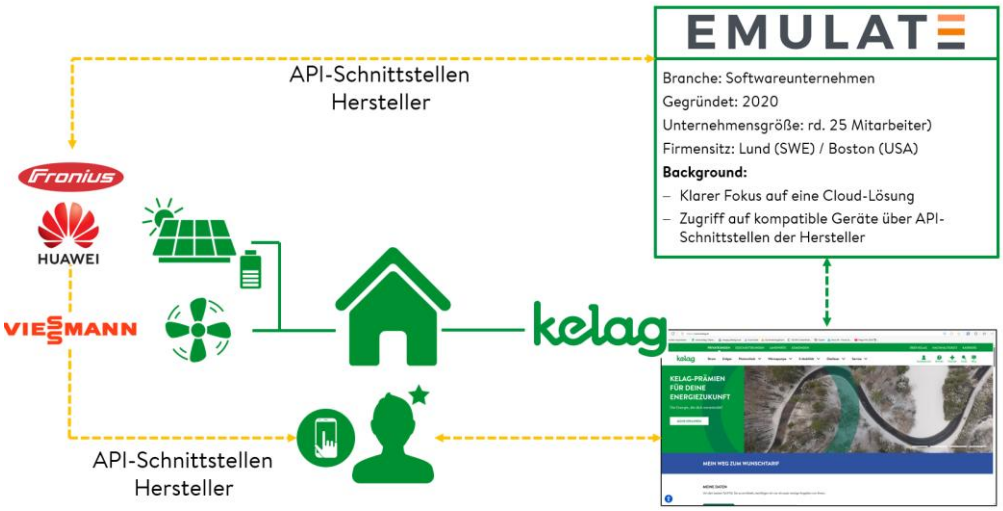


Abbildung 3.11: Onboarding der Geräte in das Emulate-System

Welche Zielsetzungen wurden verfolgt?

- Netzdienliche Steuerung von Kundenanlagen ohne Eingriff in private Installationen
- Umsetzung von Hüllkurvenvorgaben
- Erprobung cloudbasierter Kommunikation und Steuerung

Welche Architekturvariante in der Schnittstelle zum Kunden wurde umgesetzt?

Messwerteabgleich in Emulate-Cloud und Ansteuerung der Kundenanlagen mittels API

Auf welche flexiblen Einheiten wurde Einfluss genommen?

Kunden: 8 / Anlagen: 11 (Wärmepumpen (4), PV-Anlagen (7))

In welcher Form wurden die flexiblen Einheiten angesteuert?

Gesamtheit der flexiblen Einheiten in einer Anlage, Geplant wurde die Steuerung auf Anlagenebene nach Hüllkurvenabgleich.

Über welches Kommunikationsmedium wurde die DSS angebunden?

Kundeninternet für API-Anbindung der Kundenanlagen an Emulate.

Wie wurde die DSS beim Kunden installiert?

Keine zusätzliche Hardware außer Panel Server für Messung; Steuerung erfolgt über bestehende Internetverbindung des Kunden via API.

Welche Daten wurden zu welchem Zeitpunkt über die DSS ausgetauscht?

- DSS = EMULATE: Alle 10 Minuten: Messwerte von Schneider-Cloud
- Emulate verarbeitet diese und sendet Steuerbefehle nach Hüllkurvenvergleich

Gab es eine Quittierung seitens der Netzkunden?

Nach dem Onboarding brauchte der Kunde nicht mehr eingreifen. Im aktuellen Setup erfolgt keine aktive Rückmeldung durch den Kunden. Steuerung basiert auf Messwertabgleich.

In welcher Granularität wurden Daten ausgetauscht?

Die Reaktionszeit für Steuerbefehle betrug im Pilot etwa 12 Minuten. Diese Verzögerung resultierte aus dem Zusammenspiel der beteiligten Systeme:

1 Minute für die Datenabfrage von der Emulate-Cloud zur Schneider-Cloud,

10 Minuten für die Bereitstellung der Messwerte durch die Schneider-Cloud (Update alle 10 Minuten, jeweils mit zwei Zeitstempeln im 5-Minuten-Raster),

1 Minute für die Verarbeitung durch Emulate und die Auslösung der Steuerbefehle.

Eine schnellere Übertragung im Sekundenbereich wäre über ein Leitsystem wie Modbus möglich gewesen, jedoch nicht kompatibel mit der Emulate-Integration. Daher wurde eine Lösung über die jeweiligen Cloud-Systeme gewählt.

Schneider arbeitet daran, die Aktualisierungsfrequenz künftig auf 5 Minuten zu verkürzen.

Wurden Anforderungen an Cybersecurity betrachtet und welche Art der Authentifizierung gab es?

- Cloudbasierte Kommunikation mit API-Zugriff
- Authentifizierung über API-Token beim Onboarding des Kunden

Wurden mehrere gegenläufige Steuersignale / Einsatzinformationen getestet? Wenn ja, welche Prioritätsregeln wurden definiert?

Nein, im Pilot keine parallelen Steuerbefehle durch Aggregatoren oder andere Quellen.

Wo findet die Koordinierung der flexiblen Einheiten statt?

In der Emulate-Cloud, basierend auf Hüllkurvenabgleich.

Welches Monitoringkonzept wurde berücksichtigt? Wie konnte bspw. sichergestellt werden, dass die von einer flex. Einheit angeforderte netzdienliche Leistung auch am Zählpunkt angekommen ist?

- Vergleich der Messwerte mit Hüllkurve
- Steuerung erfolgt bei Abweichung
- Rückmeldung über Messwerte, keine aktive Bestätigung am Zählpunkt

Welches Update-Management ist bei der angestrebten Lösung vorgesehen bzw. denkbar? Sind Funktionserweiterungen möglich? Welche Akteure müssten eingebunden werden?

- Updates über Cloud möglich
- Funktionserweiterungen durch Emulate und Schneider denkbar

Wie resilient / robust ist die angestrebte Lösung, insb. mit Blick auf den Ausfall kritischer Infrastruktur bzw. wichtiger Komponenten? Kann ein Teilbetrieb aufrecht erhalten werden (z. B. bei dezentralen Ansätzen)? Welche Rückfallebenen sind in Situationen mit Störungen vorgesehen? Welche Fall-back-Prozesse wurden definiert? Wie anfällig ist das Lösungskonzept mit Blick auf Manipulationen, bspw. mit Blick auf ungewünschtes Netznutzerverhalten?

- Bei Ausfall der Kommunikation: Fail-Safe Verhalten möglich (z. B. max. 60 % Einspeisung)
- Manipulationsschutz durch Cloud-Authentifizierung und API-Token

Mit Blick auf die DSS: Wo werden Standardisierungsnotwendigkeiten gesehen?

- Einheitliche Schnittstellen des DSS-Portals
- Datenformate für Hüllkurven und Steuerbefehle
- Sicherheitsstandards für Kommunikation

Welche Herausforderungen sind aufgetreten? Welche Empfehlungen für die Einführung einer DSS leiten Sie aus dem Piloten ab?

Es traten hohe Latenzzeiten auf, da die Aktualisierung der Messwerte in der Schneider-Cloud nur alle 10 Minuten erfolgte. Zusätzlich gab es Probleme bei der Ansteuerung der Geräte über die API-Verbindungen.

Die Datenaktualisierung deutlich zu verkürzen (z. B. auf 5 Minuten oder weniger), um die Reaktionszeiten zu verbessern.

Eine klare Rollenverteilung und Schnittstellenbeschreibung sowie Fail-Safe Verhalten ist notwendig.

Projektspezifische Fragen:

Wodurch kommt die Reaktionszeit von ca. 12 Minuten zustande?

Die beobachtete Reaktionszeit von etwa 12 Minuten ergibt sich aus dem Zusammenspiel der beteiligten Systeme und deren Datenverarbeitung. Sie setzt sich wie folgt zusammen:

- 1 Minute für die Datenabfrage von der Emulate-Cloud zur Schneider-Cloud
- 10 Minuten für die Datenbereitstellung durch die Schneider-Cloud, die alle 10 Minuten aktualisierte Messwerte von der Messeinrichtung im Feld empfängt. Diese enthalten jeweils zwei Zeitstempel im 5-Minuten-Raster. Aufgrund der Datenmenge und Systemarchitektur ist eine schnellere Aktualisierung derzeit technisch nicht möglich. Schneider arbeitet jedoch daran, die Aktualisierungsfrequenz auf 5 Minuten zu verkürzen.
- 1 Minute für die Verarbeitung durch Emulate, bei der die Messwerte mit der Hüllkurve abgeglichen und die entsprechenden Steuerbefehle ausgelöst werden.

Zwar wäre eine schnellere Datenübertragung im Sekundenbereich (z. B. 5 oder 10 Sekunden) über ein Leitsystem wie Modbus seitens Schneider technisch möglich gewesen, jedoch konnte damit keine direkte Verbindung zu Emulate hergestellt werden. Aus diesem Grund wurde eine Lösung über die jeweiligen Cloud-Systeme gewählt.

Was war die konkrete Rolle von Emulate?

Im Rahmen des Projekts hat Emulate eine Schlüsselrolle übernommen. Über ein benutzerfreundlich gestaltetes Frontend ermöglichte Emulate die Kundenregistrierung inklusive der Erfassung und Integration steuerbarer Lasten (WP)/Photovoltaikanlagen (inkl. Speicher) über Hersteller-APIs. Dadurch war es erstmals möglich, private Betriebsmittel gezielt – also direkt am jeweiligen Netzanschlusspunkt bzw. NS-Abgang – anzusteuern. Die Einbindung verschiedenster Hersteller-APIs stellte sich jedoch als deutlich komplexer heraus, als ursprünglich angenommen und uns gegenüber kommuniziert.

Als Verteilnetzbetreiber (VNB) verfolgten wir den Ansatz, die Hüllkurve eines Netzknotens in geeigneter Form (Pilot: Excel, später evtl. Webpage) bereitzustellen. Der Aggregator – in diesem Fall Emulate – übernimmt daraufhin die Steuerung der vom Kunden freigegebenen Betriebsmittel. Daraus ergab sich die Notwendigkeit, dass Emulate auch die von uns bereitgestellte Hüllkurve verarbeiten kann.

Dabei zeigte sich: Die Hüllkurve allein reicht nicht aus, um eine zuverlässige Steuerung zu gewährleisten. Es bedarf zusätzlich der aktuellen Ist-Werte am jeweiligen Netzknoten. Aus diesem Grund wurde auch die Integration von Schneider-Messwerten notwendig (Feldmessung).

Wurde ein getrenntes Netzwerk etabliert mit dem Schneider Geräte zu Emulate zu kommunizieren, welche Folgen hatte das?

Nein, es wurde kein physisch getrenntes Netzwerk zwischen dem Schneider-Gerät und Emulate eingerichtet. Stattdessen hat der PanelServer über LTE eine Verbindung zur Schneider-Cloud aufgebaut und die Messwerte dorthin übertragen. Emulate hat diese Daten anschließend über eine API-Schnittstelle aus der Schneider-Cloud abgefragt.

Diese Architektur hatte den Vorteil, dass keine direkte Netzverbindung zwischen den beiden Systemen notwendig war. Dadurch konnten sowohl die Netzsicherheit als auch die Trennung der Verantwortlichkeiten zwischen den beteiligten Systemen gewahrt bleiben.

Warum wurde nicht auf Bestandslösungen von Schneider zu Stationsüberwachung gesetzt?

Die direkte Ansteuerung von Betriebsmitteln über bestehende Hersteller-APIs ist mit den Lösungen von Schneider nicht möglich. Zwar bietet Schneider eine HEMS-Lösung an, diese erfordert jedoch die Installation spezifischer Hardwarekomponenten in jedem einzelnen Haushalt.

Als Verteilnetzbetreiber (VNB) haben wir bewusst nach einem Ansatz gesucht, der ohne physische Eingriffe in die private Hausinstallation auskommt. Unser Ziel war es, eine Lösung zu etablieren, die keine Vor-Ort-Maßnahmen oder das Betreten privater Haushalte notwendig macht (kein Eingriff in der privaten Kundeninstallation).

3.1.8 Pilot 8: Grid Stabilizer für Netz NÖ

Involvierte Industrieunternehmen: WAGO Kontakttechnik

Laufzeit: April 2025 – September 2026 (Weiterführung nach DSS Projekt)

Beschreibung des Projektes:

Ziel des Pilotprojekts war es, die grundlegenden Funktionen einer digitalen Kundenschnittstelle anhand der Steuerung und Messung einer PV-Anlage zu erproben. Dabei wurden die im Rahmen nationaler Workshops definierten Vorgaben überprüft und in der DSS-Demo eine Echtzeitmessung der elektrischen Wurzel sowohl in der Ortsnetzstation als auch bei Endkunden umgesetzt. Die Messdaten wurden über die M-Bus-Schnittstelle der Smart Meter ausgelesen und durch die WAGO SPS verarbeitet, um Netzengpässe frühzeitig zu erkennen.

Bei den Endkunden kamen intelligente WAGO-Geräte zum Einsatz, die Messwerte erfassten und über eine Modbus TCP-Schnittstelle mit den PV-Anlagen kommunizierten. Zusätzlich wurde ein Fail-Safe-Verhalten implementiert, um bei Ausfällen einen sicheren Betriebszustand zu gewährleisten. Die Datenübertragung erfolgte über LTE, wobei SIM-Karten in den SPS-Geräten verwendet wurden. Die Trafostations-SPS übermittelte Messwerte und empfing Berechnungsergebnisse aus der Cloud, während die Endkunden-SPS Leistungsvorgaben an die PV Anlagen weitergaben. Neben präventiven Eingriffen auf Basis von Prognose-Hüllkurven wurden auch kurative Maßnahmen berücksichtigt, um auf unvorhergesehene Netzsituationen in Echtzeit reagieren zu können.

Im Pilotversuch wurden zentrale Erkenntnisse zur Installation und zum Betrieb der DSS-Funktionsblöcke sowie zur digitalen Schnittstelle gewonnen. Drahtlose Kommunikation bei Endkunden

erwies sich als praktikabel und empfehlenswert, wodurch der Verdrahtungsaufwand reduziert werden konnte. Die Wirkleistungsvorgabe an den DSS-Block war grundsätzlich möglich, ihre Umsetzung hing jedoch vom Verhalten der Wechselrichter ab. Hybridanlagen ohne EMS konnten keine zählpunktscharfen Vorgaben umsetzen, was zu Kundenbeschwerden führte – EMS wurden daher als Standard empfohlen. Die Spannungsversorgung des Smart Meter Adapters über M-Bus war unzuverlässig, weshalb Netzteile notwendig waren, die jedoch meist nicht im Verteiler vorhanden waren. Der Betrieb des Adapters im Access Point Modus verursachte Systemausfälle, sodass eine stabile WLAN-Integration erforderlich wurde.

Zudem zeigte sich, dass der Adapter zwar die einzige Möglichkeit zur Echtzeitauslesung darstellte, jedoch fraglich blieb, ob VNB diese Daten tatsächlich benötigen. Die Hardware des Funktionsblocks erforderte zusätzlichen Platz und war nur vor Ort austauschbar, was eine robuste Rollout-Lösung notwendig machte. Die Installation musste durch Elektrofachkräfte erfolgen, sollte aber möglichst einfach gehalten sein – eine Plug-and-Play-Lösung wäre empfohlen. Für die digitale Schnittstelle wäre eine Cloudlösung bevorzugt, bei der VNB Parameter und Hüllkurven senden und Endkunden-EMS diese abrufen. Standardisierte Schnittstellen und eine gemeinsame Entwicklung durch Netzbetreiber wurden als essenziell erkannt, wobei sowohl zentrales als auch dezentrales Hosting möglich wäre.

Die Einführung einer digitalen Schnittstelle wurde als zentraler Erfolgsfaktor für die Umsetzung von Flexibilitätskonzepten erkannt. Sie muss national einheitlich, robust und standardisiert konzipiert sein – inklusive klarer Protokolle, definierter Prozesse, sicherer Authentifizierung und Anbindung an Netzbetreiberportale – wobei eine Cloudlösung als bevorzugter Weg gilt.

Schaubild der Kommunikation zwischen den Akteuren:

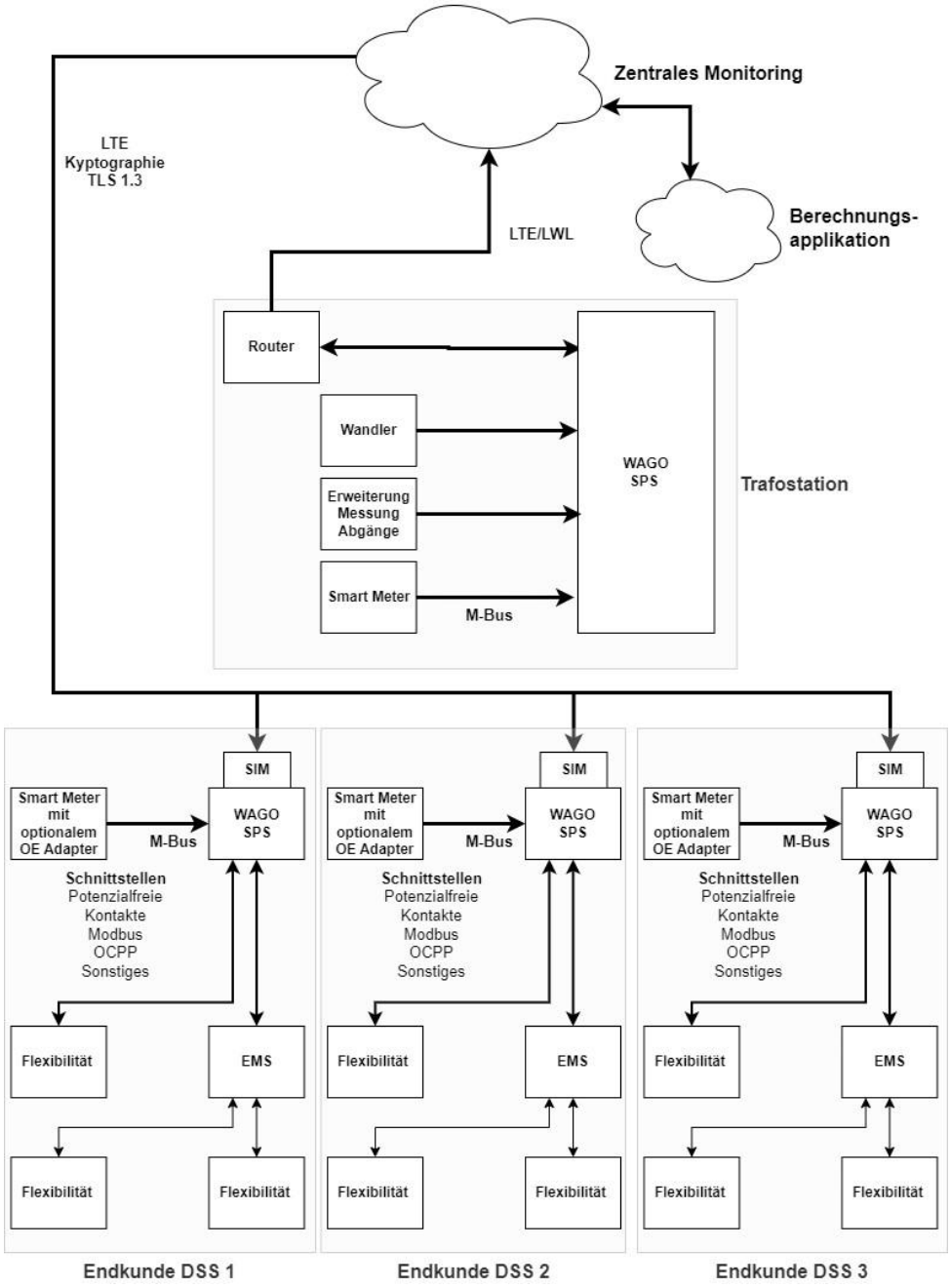


Abbildung 3.12: Schaubild von Pilot Grid Stabilizer

Welche Zielsetzungen wurden verfolgt?

Vorgaben von Leistungsvorgaben an PV bei kritischer Einspeisesituation + Auslesung der Aktivierung über Echtzeit Messwerte

Welche Architekturvariante in der Schnittstelle zum Kunden wurde umgesetzt?

Funktionsblock Hardware mit eigener Software

Auf welche flexiblen Einheiten wurde Einfluss genommen?

PV: 2 Kundenanlagen; Umsetzbar war aufgrund von Problemen nur eine

In welcher Form wurden die flexiblen Einheiten angesteuert?

Einzelne Flexible Einheiten einer Anlage (kein EMS vorhanden)

Über welches Kommunikationsmedium wurde die DSS angebunden?

Mobilfunk über MQTT (S)

Wie wurde die DSS beim Kunden installiert?

Funktionsblock in Kundenverteiler. Verbindung über Kunden WLAN mit Smart Meter Adapter und PV Wechselrichter

Welche Daten wurden zu welchem Zeitpunkt über die DSS ausgetauscht?

Präventiv bereits umgesetzt, kurativ folgt

Gab es eine Quittierung seitens der Netzkunden?

Übermittlung der Messwerte, Empfangs und Vollzugsmeldung

In welcher Granularität wurden Daten ausgetauscht?

Echtzeitdaten wurden übermittelt. Durch hohen Datenaufwand wollen wir bei Rollout davon absehen und Hauptanteil präventiv umsetzen.

Wurden Anforderungen an Cybersecurity betrachtet und welche Art der Authentifizierung gab es?

Passwort, Zertifikat

Wurden mehrere gegenläufige Steuersignale / Einsatzinformationen getestet? Wenn ja, welche Prioritätsregeln wurden definiert?

Nein, nur Vorgaben durch VNB

Wo findet die Koordinierung der flexiblen Einheiten statt?

Separate Instanz: Cloud Berechnungsplattform des Ortsnetzes (WAGO Grid Stabilizer)

Welches Monitoringkonzept wurde berücksichtigt? Wie konnte bspw. sichergestellt werden, dass die von einer flex. Einheit angeforderte netzdienliche Leistung auch am Zählpunkt angekommen ist?

Monitoring über Smart Meter Adapter Verbindung zu FB. Darstellung am Grid Gateway und Grafana für Tests

Welches Update-Management ist bei der angestrebten Lösung vorgesehen bzw. denkbar? Sind Funktionserweiterungen möglich? Welche Akteure müssten eingebunden werden?

WAGO Solution platform, Erweiterungen per update möglich, SW Entwicklungsabteilung. Ziel wäre einzelne Verbindung an EMS. FB durch hohe intelligenz erweiterbar

Wie resilient / robust ist die angestrebte Lösung, insb. mit Blick auf den Ausfall kritischer Infrastruktur bzw. wichtiger Komponenten? Kann ein Teilbetrieb aufrecht erhalten werden (z. B. bei dezentralen Ansätzen)? Welche Rückfallebenen sind in Situationen mit Störungen vorgesehen? Welche Fall-back-Prozesse wurden definiert? Wie anfällig ist das Lösungskonzept mit Blick auf Manipulationen, bspw. mit Blick auf ungewünschtes Netznutzerverhalten?

NIS 2 konform, einstellbare fall back Ebene. Dezentrale Ansätze sind denkbar. Fallback Szenario bei Ausfall umsetzbar. Wichtig ist, dass auch der Wechselrichter reagiert. Manipulationssicherheit ist gegeben.

Mit Blick auf die DSS: Wo werden Standardisierungsnotwendigkeiten gesehen?

Kommunikation zu den Flexibilitäten.

Standard Protokoll für Anbindung Endgeräte an DSS. Standard Onboarding und Offboarding Prozesse.

Standard Validierungsprozesse (Abruf der Hüllkurven), Implementierung der Grund Funktionalitäten bei jedem VNB gleich. EMS als Standard ab Leistung > 7kW

Welche Herausforderungen sind aufgetreten? Welche Empfehlungen für die Einführung einer DSS leiten Sie aus dem Piloten ab?

Fehlende Doku Smart Meter Adapter, IT Zugang Endkunde

Hardwareaufwand als Schwierigkeit: Vieles von Softwareseite lösen zu empfehlen.

Behind the meter assets: EMS als Standard notwendig für zählpunkt scharfe Vorgaben

Skalierbarkeit: Mit der DSS zusammenhängende Prozesse müssen standardisiert werden

Vereinheitlichung: jeder Pilot mit unterschiedlichem Scope → in der DSS in einem Standard vereinen

Projektspezifische Fragen:

Wie war die Erfahrung der MQTT-Verbindung zwischen Kunde und Netzbetreiber?

Erfahrungen sind hier durchaus positiv. Durch Aufsetzen eines MQTT Brokers im FB konnten die Kunden Geräte robust angebunden werden. MQTT wird laut unserer Fachabteilung wegen seiner Einfachheit leichter zu warten sein, und weniger hochspezialisiertes Nischenwissen voraussetzen.

Gab es Schwierigkeiten mit dem Hardware-Block?

Platzthematik und Versorgung des Adapters… spricht gegen eine Umsetzung im eigenen Gerät,

Platzthematik für den Funktionsblock: Hier muss es einen freien Zählerplatz für die Hardware geben. Als Alternative wäre auch eine Ausführung im Kunden Wohnbereich denkbar. Voraussetzung wäre Berührungssicherheit (abgekapselt). Vorteil wäre hier der Empfang und die Einfachere Installation. (Power Grid User Interface von Areti bietet hier eine elegante Lösung für den FB einer digitalen Schnittstelle).

Bei beiden Varianten wäre es wünschenswert, nur eine sofwaretechnische Verbindung zu EMS oder sonstigen Komponenten herstellen zu müssen.

Platzthematik für den Adapter war Nebensache – wenn Platz für einen Funktionsblock ist, dann ist auch Platz für den Adapter.

Funktionsblock WLAN Konfiguration … auch ähnliche Problematik zu Problemen im Schaltschrank wie im Projekt oPenGrid4PV

Problem war hier die Konfiguration des Smart Meter Adapters. Dieser fiel im Access Point Modus öfter aus. Bei jedem Ausfall wurde die MQTT Schnittstelle deaktiviert. Hier wäre eine Verbesserung des Adapters oder eine Integration im Smart Meter 2.0 (je nach Mehrkosten) wünschenswert

Der FB selbst hatte keine Probleme mit der Konfiguration. WLAN oder Mobilfunk Empfang ist jedoch Voraussetzung. Dieses Problem könnte mit der Installation der Hardware im Wohnraum

umgesetzt werden. Langfristig ist es auch wahrscheinlich, dass Kunden mit einem EMS auch eine WLAN Verbindung zu diesem herstellen.

3.1.9 Pilot 9: OpenGrid4PV für EWE & E-Werk Perg

Involvierte Industrieunternehmen: Reisenbauer, Sticon

Laufzeit: 03/2024 – 08/2026

Beschreibung des Projektes:

Ausgangssituation, Problematik und Motivation: Um die österreichischen Klimaziele bis 2030 (100 % Strom aus Erneuerbaren bis 2030) zu erreichen, ist ein massiver Ausbau der PV-Leistung um 11 GWpeak erforderlich, Oberösterreich alleine sich 3500 MWpeak installierter Leistung als Ziel bis 2030 gesetzt. Aber bereits jetzt ist in vielen Gemeinden aufgrund ausgelasteter Umspannwerke und überlasteter Niederspannungsnetze keine zusätzliche PV-Einspeisung mehr möglich, was großen Unmut in der Bevölkerung hervorruft und auch den notwendigen Ausbau der Photovoltaik zur Erreichung der Klimaschutzziele des Landes und des Bundes erschwert bzw. verhindert, die ohne kurzfristig anwendbare Alternativen zum langwierigen Netzausbau nicht erreichbar sein werden.

Ziele und Innovationsgehalt:

Das vorliegende Projektvorhaben zielt daher auf die Entwicklung anwendbarer, kostengünstiger, zeitnah umsetzbarer und gesellschaftlich tragfähiger Lösungsansätze zur Erhöhung der PV-Hosting Capacity bzw. zur effizienteren Nutzung vorhandener Kapazitäten in Nieder- und Mittelspannungsnetzen ab.

Dazu werden in gemeinsamen Co-Creation-Workshops mit den betroffenen Stakeholdern (z. B. NetzbetreiberInnen, EndkundInnen, E-Control, …) deren individuelle Anforderungen und Bedürfnisse erhoben und darauf aufbauend entsprechende Lösungsansätze und Konzepte unter Berücksichtigung zukünftiger Entwicklungen (z. B. bidirektionales Laden) entwickelt. Diese Lösungsansätze werden in der Folge mittels Simulation validiert (Funktionalität, Beitrag zur Zielerreichung, Effizienz, Skalierbarkeit…) und unter anderem rechtlich/regulatorisch geprüft. Vielversprechende anwendbare Lösungsansätze werden in der Folge in ausgewählten Netzabschnitten, in denen es bereits jetzt Probleme gibt, getestet und bei Bedarf angepasst um deren Machbarkeit zu demonstrieren und zur Nachahmung anzuregen.

Großer Wert wird dabei auf eine verständliche, breitenwirksame Kommunikation sowie Partizipation gelegt, mit dem Ziel die Bevölkerung zu informieren und aktiv einzubinden, dabei zu helfen Zusammenhänge zu verstehen sowie Verständnis und Bewusstsein für aktuelle Herausforderungen zu schaffen, um damit deren Akzeptanz und Bereitschaft zu erhöhen.

Angestrebte Ergebnisse und Erkenntnisse des Projekts sind

- anwendbare, kostengünstige, zeitnah umsetzbare und gesellschaftlich tragfähige Lösungsansätze zur Erhöhung der PV-Hosting Capacity bzw. zur effizienteren Nutzung vorhandener Kapazitäten in Nieder- und Mittelspannungsnetzen zu erwarten, die
- technisch, gesellschaftlich, ökonomisch sowie rechtlich/regulatorisch geprüft und deren Machbarkeit in einem realen Umfeld demonstriert wurde und
- die aufgrund der Mitwirkung der Bevölkerung eine hohe Akzeptanz aufweisen.

Schaubild der Kommunikation zwischen den Akteuren:

Variante 2, DSS: 1 (DSS ist eigenes Gateway)

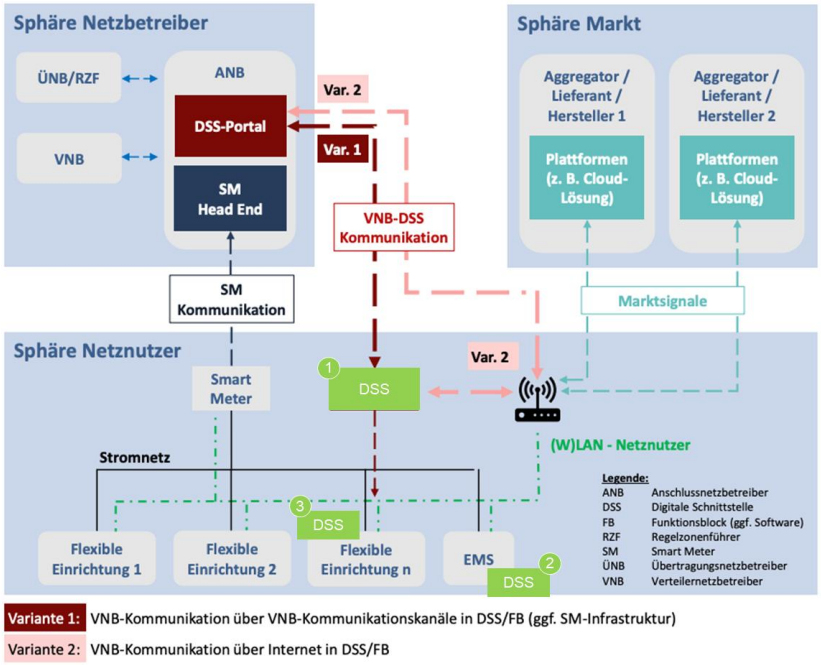


Abbildung 3.13: Schaubild von Pilot OpenGrid4PV

Welche Zielsetzungen wurden verfolgt?

Demonstration von Lösungen und Regelungsstrategien zur Steigerung der PV-Einspeisung bei gleichzeitigem Erhalt der Netzstabilität

Welche Architekturvariante in der Schnittstelle zum Kunden wurde umgesetzt?

Funktionsblock: Hardware mit eigener Software

Auf welche flexiblen Einheiten wurde Einfluss genommen?

Wechselrichter und Batteriespeicher

Zwei Testbeds: 5 bzw. 3 Kundenanlagen

In welcher Form wurden die flexiblen Einheiten angesteuert?

Einzelne flexible Einheit einer Anlage

Über welches Kommunikationsmedium wurde die DSS angebunden?

Kunden-Internet

Wie wurde die DSS beim Kunden installiert?

Einbau eines Controllers (Messung der Netzanschlussleistung und Steuerung der Komponenten) im Niederspannungsverteiler durch Elektriker und Integration ins Heimnetzwerk durch Techniker

Welche Daten wurden zu welchem Zeitpunkt über die DSS ausgetauscht?

Bisher nur kurative Regelung durch Vorgabe der Einspeiseleistung/Einspeisebegrenzung

Gab es eine Quittierung seitens der Netzkunden?

Reaktion kann auf Basis der übermittelten Messungen am Netzanschlusspunkt bewertet werden.

In welcher Granularität wurden Daten ausgetauscht?

Es wurde versucht nahe Echtzeit zu arbeiten. Die tatsächliche Latenzzeit konnte bisher noch nicht final erprobt werden.

Wurden Anforderungen an Cybersecurity betrachtet und welche Art der Authentifizierung gab es?

Keine Antwort des Piloten

Wurden mehrere gegenläufige Steuersignale / Einsatzinformationen getestet? Wenn ja, welche Prioritätsregeln wurden definiert?

Wurde bisher nicht getestet.

Wo findet die Koordinierung der flexiblen Einheiten statt?

Kunden erhalten Anforderung an die Einspeisebegrenzung und Wechselrichter (EMS) sollen diese umsetzen.

Welches Monitoringkonzept wurde berücksichtigt? Wie konnte bspw. sichergestellt werden, dass die von einer flex. Einheit angeforderte netzdienliche Leistung auch am Zählpunkt angekommen ist?

Kann durch Live-Messdaten an Netzanschlusspunkt und Wechselrichter gemonitort / sichergestellt werden.

Welches Update-Management ist bei der angestrebten Lösung vorgesehen bzw. denkbar? Sind Funktionserweiterungen möglich? Welche Akteure müssten eingebunden werden?

Es muss lediglich der Controller upgedatet werden. Funktionserweiterungen sind einfach umsetzbar, da die Regelungsstrategie zentral programmiert wird. Neue Funktionen können durch Reisenbauer umgesetzt werden.

Wie resilient / robust ist die angestrebte Lösung, insb. mit Blick auf den Ausfall kritischer Infrastruktur bzw. wichtiger Komponenten? Kann ein Teilbetrieb aufrecht erhalten werden (z. B. bei dezentralen Ansätzen)? Welche Rückfallebenen sind in Situationen mit Störungen vorgesehen? Welche Fall-back-Prozesse wurden definiert? Wie anfällig ist das Lösungskonzept mit Blick auf Manipulationen, bspw. mit Blick auf ungewünschtes Netznutzerverhalten?

Kommunikationsausfälle werden folgendermaßen abgefangen:

- Unterbrechung zwischen Server und Controller: Controller führt Komponenten in lokales Backup zurück (statische Einspeisebeschränkung)
- Unterbrechung zwischen Controller und Komponenten: Komponenten haben Fallback-Setpoints im Falle eines Ausfalls der Kommunikation im lokalen Netzwerk.

Robustheit gegenüber ungewünschtem Netznutzerverhalten wurde noch nicht geprüft.

Mit Blick auf die DSS: Wo werden Standardisierungsnotwendigkeiten gesehen?

Authentifizierung (obwohl dieser Punkt im vorliegenden Piloten nicht untersucht wurde)

Nachrichtenformat/Inhalt

Welche Herausforderungen sind aufgetreten? Welche Empfehlungen für die Einführung einer DSS leiten Sie aus dem Piloten ab?

- Verlässlichkeit des lokalen Netzwerkes oft problematisch
- Einbau des Controllers aufwändig (Elektriker nötig)

- Fallback-Werte (statische Einspeisung) sollten trotz Steuerung auf die lokal zulässige Einspeiseleistung gesetzt werden. Ein Kommunikationsausfall könnte sonst zu unerwartet hohen Leistungsgradienten führen
- Oftmals keine direkte Vorgabe der netzwirksamen Einspeiseleistung möglich, sondern nur der max. Wechselrichterleistung

3.1.10 Pilot 10: Friendly Charge für Energienetze Steiermark

Involvierte Industrieunternehmen:

- Montanuniversität Leoben
- Technische Universität Wien
- AIT Austrian Institute of Technology GmbH
- Energie Steiermark AG
- E-VO eMobility GmbH
- Siemens Aktiengesellschaft Österreich

Laufzeit: 01.03.2023 – 28.02.2026 (Verlängerung beantragt)

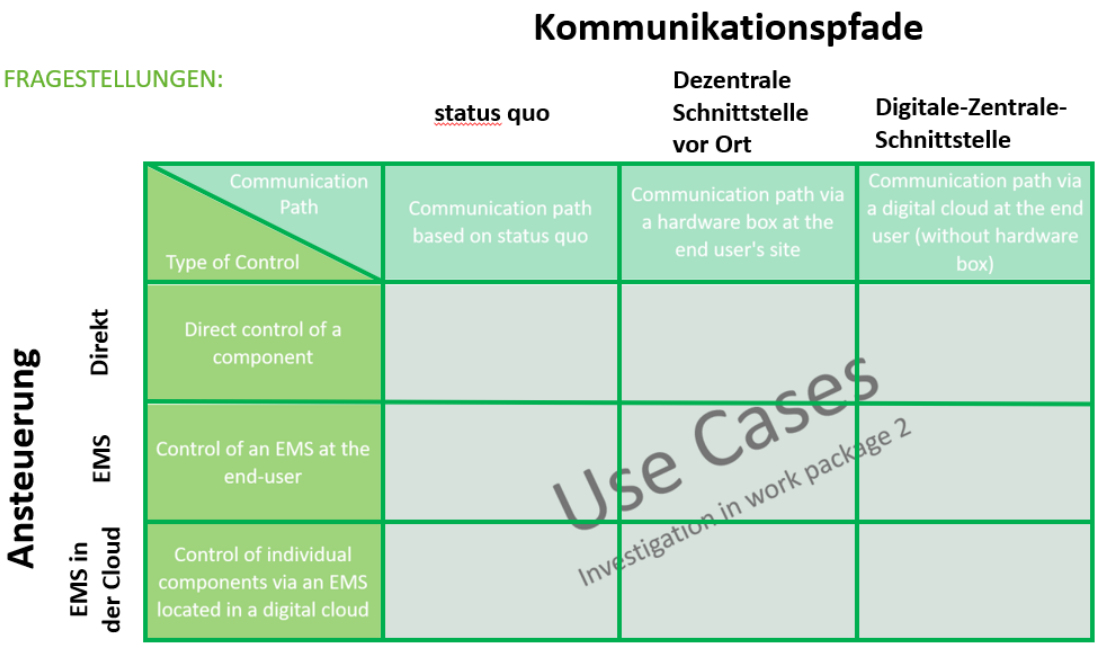
Beschreibung des Projektes:

Das übergeordnete Ziel des Projektes **friendlyCharge** ist die Entwicklung und Demonstration eines Kundenschnittstellen-Prototyps, um sicheres, bedarfsgerechtes und netzfreundliches Laden in Wohngebieten zu ermöglichen und die Integration aller Arten von Ladestationen so zu gestalten, dass der Ladebedarf möglichst vollständig mit dem vorhandenen Netzressourcen gedeckt werden kann.

Zu diesem Zweck wird eine innovative Schnittstelle für die Kommunikation zwischen Netz und Nutzern (nahezu) in Echtzeit entwickelt und demonstriert. Neben dem technischen Konzept befasst sich das Projekt mit Anforderungen im Bereich der Kommunikationssicherheit sowie den rechtlichen und regulatorischen Rahmenbedingungen.

Zur Zielerreichung werden im Projekt verschiedene Ansteuerungsarten und Kommunikationswege untersucht: Die Schnittstelle kann direkt (über Smart Meter Schaltkontakt), über ein ansteuerbares Device vor Ort oder cloudbasiert angesteuert werden.

FRAGESTELLUNGEN:



Dazu werden drei Steuerungsarten der Kundenschnittstelle und drei Möglichkeiten von Kommunikationspfaden definiert, was zu neun zu untersuchenden Anwendungsfällen führt. Im Rahmen des Projektes werden alle neun Use Cases (UC) in einer ersten Analyse im Hinblick auf Design, rechtliche, regulatorische und Netzwerksicherheitsaspekte untersucht. Basierend auf dieser Klassifizierung wird mindestens ein Anwendungsfall als Demonstrator für die Umsetzung identifiziert und die Kundenschnittstelle als Prototyp für den identifizierten Einsatz entwickelt.

Weitere Anwendungsfälle werden beispielsweise im Hinblick auf die Netzwerk Sicherheit untersucht.

Die Demonstration erfolgt im Niederspannungsnetz der Energienetze Steiermark und umfasst sowohl Labor- als auch Feldtests und ist mit mehreren Pilotkunden und unterschiedlichen Ladestationsarchitekturen vorgesehen.

Schaubild der Kommunikation zwischen den Akteuren:

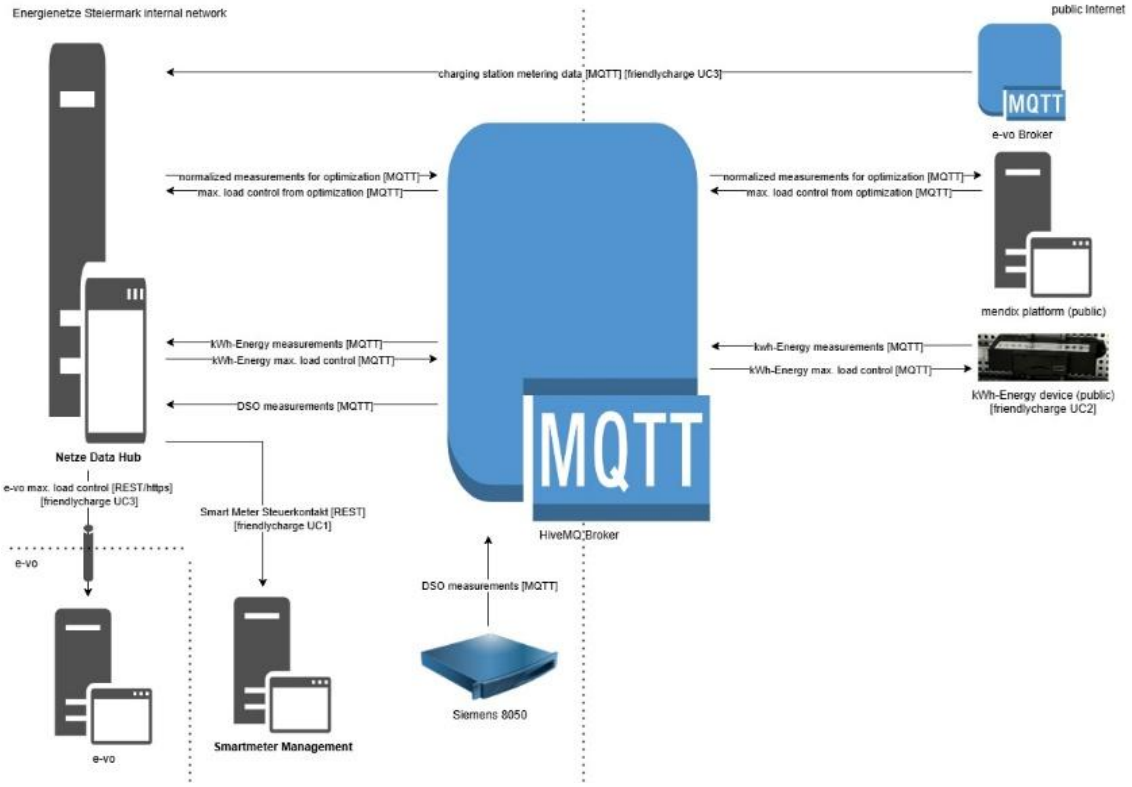


Abbildung 3.14: Schaubild von Pilot Friendly Charge

Welche Zielsetzungen wurden verfolgt?

Entwicklung und Demonstration eines Kundenschnittstellen-Prototyps, um sicheres, bedarfsgerechtes und netzfreundliches Laden in Wohngebieten zu ermöglichen und die Integration aller Arten von Ladestationen so zu gestalten, dass der Ladebedarf möglichst vollständig mit dem vorhandenen Netzressourcen gedeckt werden kann.

Welche Architekturvariante in der Schnittstelle zum Kunden wurde umgesetzt?

Funktionsblock: Hardware mit eigener Schnittstelle (Use Case 2a)

Schnittstelle im EMS des Kunden (Use Case 2b)

Sonstige: über einen Aggregator (Use Case 3a)

Auf welche flexiblen Einheiten wurde Einfluss genommen?

Ladestationen / Mehrere verschiedene Wallboxen / Mehrere Pilotkunden

In welcher Form wurden die flexiblen Einheiten angesteuert?

Wir steuern die Gesamtheit der flexiblen Einheiten in einer Anlage (Ladestationen)
Im UC 3a ist die Gesamtheit eine Ladebox

Über welches Kommunikationsmedium wurde die DSS angebunden?

UC 3 - Rest API - EVO (VPN, Internet)

UC 2 - MQTT (Internet)

Wie wurde die DSS beim Kunden installiert?

UC 2 – eigene Hardware

UC 3 – ohne Hardware vor Ort, über Aggregator (EVO)

Welche Daten wurden zu welchem Zeitpunkt über die DSS ausgetauscht?

Leistungslimits, Hüllkurve

Gab es eine Quittierung seitens der Netzkunden?

Nachdem der Kunde seine Zustimmung für den Zugriff gegeben hat, war es möglich im Projekt auf die Ladestationen zuzugreifen.

In welcher Granularität wurden Daten ausgetauscht?

Die Siemens EGS-Messgeräte können Daten im 10 Sekunden Takt senden und messen Spannungen, Ströme und berechnen die Wirk- und Blindleistung sowie den Phasenwinkel.

Wurden Anforderungen an Cybersecurity betrachtet und welche Art der Authentifizierung gab es?

Im Rahmen des Projekts wurde der eingesetzte **MQTT-Broker** gemäß den Vorgaben der **NIS2-Richtlinie** eingerichtet. Verwendete Schnittstellen werden entsprechend der Möglichkeiten hinsichtlich Authentifizierung und Verschlüsselung eingesetzt. Die Anbindung von Kundengeräten erfolgt über die Authentifizierung mit Zertifikaten (UC2) bzw. über gesicherte Kanäle (UC3)

Wurden mehrere gegenläufige Steuersignale / Einsatzinformationen getestet? Wenn ja, welche Prioritätsregeln wurden definiert?

Der Netzbetreiber hat bei unserem Ansatz immer Priorität

Wo findet die Koordinierung der flexiblen Einheiten statt?

Mehr als eine Einheit müssen bei unserem Ansatz immer über ein EMS koordiniert werden

Welches Monitoringkonzept wurde berücksichtigt? Wie konnte bspw. sichergestellt werden, dass die von einer flex. Einheit angeforderte netzdienliche Leistung auch am Zählpunkt angekommen ist?

Es gibt einen privaten Energiemeter am Netzanschlusspunkt. Zusätzlich existiert aus einem Vorprojekt eine Messstelle auf der Netzseite

Welches Update-Management ist bei der angestrebten Lösung vorgesehen bzw. denkbar? Sind Funktionserweiterungen möglich? Welche Akteure müssten eingebunden werden?

Da es sich derzeit um einen **Piloten** handelt, wurde ein Update-Management bislang nicht berücksichtigt. Updatemanagement und Funktionserweiterungen sind in Absprache zwischen VNB und Hersteller möglich.

Das Updatemanagement könnte zukünftig auch über ein SLA geregelt werden. Je nachdem, wie sich die Entwicklung der digitalen Schnittstelle österreichweit gestaltet, werden mögliche Funktionserweiterungen von den Ergebnissen des Pilotprojekts abhängig gemacht und in Abstimmung mit den beteiligten Herstellern geplant.

Wie resilient / robust ist die angestrebte Lösung, insb. mit Blick auf den Ausfall kritischer Infrastruktur bzw. wichtiger Komponenten? Kann ein Teilbetrieb aufrecht erhalten werden (z. B. bei dezentralen Ansätzen)? Welche Rückfallebenen sind in Situationen mit Störungen vorgesehen? Welche Fall-back-Prozesse wurden definiert? Wie anfällig ist das Lösungskonzept mit Blick auf Manipulationen, bspw. mit Blick auf ungewünschtes Netznutzerverhalten?

Es werden Fallback Werte übergeben, die beim Verbindungsausfall eingehalten werden müssen.

Mit Blick auf die DSS: Wo werden Standardisierungsnotwendigkeiten gesehen?

Beim Protokoll zwischen Netzbetreiber und Netznutzer und den zu übermittelnden Daten. Gegebenenfalls sollen auch die Architekturvarianten österreichweit einheitlich umgesetzt werden und es soll zu einer einheitlichen Definition von dynamischer Regelung kommen – z.B. was bedeutet dynamisch, ist auch schon eine saisonale Steuerung zum Beispiel dynamisch.

Welche Herausforderungen sind aufgetreten? Welche Empfehlungen für die Einführung einer DSS leiten Sie aus dem Piloten ab?

IT-Anforderungen und IT Sec, rechtliche und regulatorische Situation.

Der MQTT Broker wurde IT/OT-sicher aufgebaut, um im realen Betrieb eingesetzt zu werden. Dies verzögerte den Projektablauf deutlich.

Das Projekt wurde in Absprache mit dem Konsortium bis Herbst 2026 verlängert. Dies ermöglicht es speziell auf das Thema IT Security weiter einzugehen und die im Dokument angesprochen Punkte noch weiter auszuarbeiten.

Projektspezifische Fragen:

Beschreibung der Funktionsweise des kWh.Energy und kWh.GridXpert GOI

Die Grid Operator API von kWh Energy nutzt MQTT als Transportprotokoll und kommuniziert dabei über mehrere Topics auf Basis von JSON-Daten mit dem MQTT-Broker des Netzbetreibers. Dieser muss dabei nach aktuell geplantem Einsatz öffentlich nutzbar sein, um eine Verbindung über das Kunden-Internet bzw. eine öffentliche Mobilfunkverbindung zu ermöglichen. Die Kommunikation nutzt Mutual TLS für Verschlüsselung und Authentifizierung.

Protokoll für Kommunikation mit Grid Operator API / Refresh Rate / Ausgehende Verbindung?

Messdaten werden dabei aktuell in 5 Sekunden Intervallen zum Broker übertragen, Leistungsvorgaben können On Demand über den Broker an die kWh Energy Module übermittelt werden.